EXHIBIT H

Client Workplace Policies

Commonwealth of Massachusetts

Information Technology Division

Workplace

Policies and Procedures Guide

Published 11/1/2010

Versions

Date Published	Version Number	Summary of Changes
11/1/2010	FY10.1	Policy Documents published as Appendices Update to Attendance and Hours of Work Added Guidelines for Managing Contractors Added Section on Investigations of Workplace Misconduct Added Section on Solicitation of Charitable Donations Added Section on Mother's Room Accommodations Added Section on Out of State Travel Authorization
4/21/09	FY09.2	Minor update to Desktop Unit Management Policy
11/18/08	FY09.1	Original

Section 1: Introduction

1.1 Welcome to the Information Technology Division

This workplace policy and procedures guide provides a summary of the major benefit programs and policies for employees.

Please note that this handbook was prepared as a guide for employees of this agency. The CIO can, at his or her discretion, implement and change internal policies and practices. This manual is current as of the publication date. As internal, contractual, state or federal policies and procedures change in the future, employees will be notified and appropriate updates will be made to the guide.

We hope that this valuable source of information, now available at your fingertips, will help you find answers to your most frequently asked questions. However, we must caution you that this manual is not the definitive source of answers to how the Commonwealth and the Information Technology Division operate. Because of the myriad of rules, regulations, policies, procedures and bulletins governing state employees, it is virtually impossible to adequately cover every subject. If you have further questions, we encourage you to contact the Human Resource Office and/or your appropriate collective bargaining agreement. When these guidelines conflict with existing contractual agreements, such contractual agreements shall prevail.

It is our intent to keep this information as up-to-date as possible, so that both current employees and new employees to the state will benefit from this central source of information. There will be a link to the manual on the employee portal.

We hope you find this manual useful and encourage any comments/suggestions to improve future editions.

1.2 ITD Mission Statement

The mission of the Information Technology Division is to enable state government to better serve the public through the strategic use of technology.

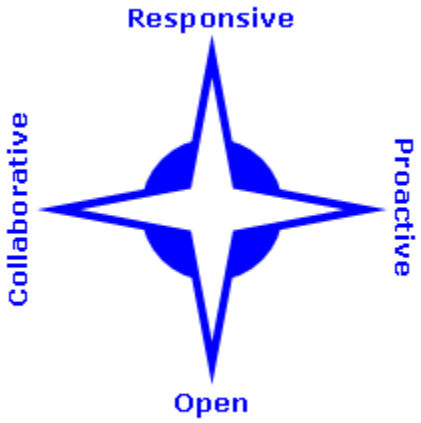
1.3 ITD Team Values

Responsive - Service-oriented attitude—"Your-problem-is-my-problem" approach, take ownership, be accountable—escalate when necessary, "can-do/will-do" mind-set, rapid follow up

Proactive - Forward thinking, take initiative to meet goals and exceed expectations

Collaborative - Team player—focus on shared goals, shared credit, shared information—positive, enjoyable work environment

Open - Continuous learner—adaptable to change—feeling safe being honest through constructive feedback, mutual respect for individuals



1.4 About ITD

The Information Technology Division (ITD) enables agencies to deliver high quality, efficient and effective services to their customers, by providing a range of centralized IT services; overseeing IT policies, standards and architecture; and promoting cross-agency collaboration and adoption of shared services. The Division is part of the Executive Office of Administration and Finance and is headed by the Commonwealth Chief Information Officer. The CCIO also chairs the ITD Executive Committee who establishes the strategic direction and priorities for the agency.

With the exception of Mass.Gov, ITD does not serve the public directly. While the agencies work directly with their customers, ITD works with the agencies as a service provider to ensure their customers' needs are met. Most services offered by ITD are processed through direct chargeback.

1.5 Office of the Chief Information Officer

The Chief Information Officer of the Commonwealth of Massachusetts, under the Executive Office for Administration and Finance, has the responsibility to set information technology standards; review and approve secretariat and department information technology strategic plans; be involved in the planning, design, and operation of information technology systems and manage central information technology systems.

The following offices within the Office of the CIO provide support functions to ITD and provide IT consultation, guidance and enterprise services to other agencies:

Finance

The Finance Office manages the overall accounting, financial reporting and financial services of the Information Technology Division. This includes managing internal controls to mitigate risk; creating and presenting financial status and financial condition reports to internal and external parties, and providing high-quality financial information that supports the Division's strategic management initiatives. In order to accomplish this, the Finance Office:

- Processes all procurements, contracts, accounts receivables and accounts payables
- Establishes the chargeback cost allocation plans and the billing/rate structure of the program

Office of the General Counsel

The mission of the General Counsel's Office is to provide technology law services to ITD and on request to other Executive Department agencies and parts of state government, as well as to counsel ITD in general legal matters. The General Counsel's office provides legal advice regarding:

- Information technology and telecommunications transactions such as technology license, maintenance, hosting, internet services, and system development and implementation agreements

- Intellectual property and electronic privacy, security, signatures, records, and accessibility
- Standard agency legal affairs related to agency authority; procurement law; responses to public records requests, subpoenas, summons and other legal process; labor and employment matters; legislation; and policy development

Human Resources

The Human Resources Office is responsible for recruitment and staffing, benefits and payroll administration, policy directives, labor relations and organizational development initiatives for ITD. In addition to these functions, the Director of Human Resources works with Secretariat CIOs to establish guidelines for IT salaries state-wide and to assist with IT recruiting and retention issues, and in collaboration with the Operational Services Division, establishes hourly rates and tracks state-wide spending on IT contractors. In order to accomplish this, the Human Resources Office:

- Contributes to ITDs operational effectiveness by improving communication at every level; including management of the ITD employee portal
- Documents and enhances HR processes
- Ensures consistency of policy compliance and management practices across ITD
- Manages the Commonwealth IT University training collaborative with UMASS

1.6 Application Services

The **Applications Office** (AO) is responsible for a host of enterprise services critical to the efficient functioning of state government. The Office focuses on providing robust, stable and cost efficient applications with a particular emphasis on customer service. The Applications Office consists of two of ITD's four lines of business; Application Services and Workgroup Services. The offices that are included in these two lines of business are detailed below:

Assistive Technology

The mission of the Assistive Technology Office is to ensure that all information technology deployed by ITD or any other Executive Branch Agency is fully accessible to and usable by persons with sensory, physical, learning, cognitive and other disabilities. In order to accomplish this, the Assistive Technology Office:

- Establishes and manages links between ITD, assistive technology vendors, hardware/software vendors, standards bodies, and disability community stakeholders
- Provides assistive technology guidance, training, direction and oversight for the development, procurement, testing and deployment of information technology
- Assures compliance with published Enterprise Information Technology and Web Accessibility Standards and Policies

Enterprise Systems Service/Middleware

The Enterprise Systems Services Office provides development, maintenance, enhancements, and 7x24x365 production support for enterprise wide applications. Currently, this portfolio includes the Human Resources Compensation Management System (HRCMS) and Commonwealth Information Warehouse (CIW). In order to accomplish this, the Enterprise Systems Services Office:

- Processes the payroll for 77,000 employees within 149 departments by means of Commonwealth of Massachusetts government policies
- Maintains enterprise wide data for the Commonwealth of Massachusetts' financial, human resource and payroll systems
- Supports approximately 6,000 end users for HRCMS and CIW

The Middleware Office enables the delivery of middleware solutions and support for customer business and enterprise shared services. In order to accomplish this, the Middleware Office:

- Provides services related to migrating mainframe applications to client/server applications
- Provides functional set of APIs over and above the operating system and network services to allow an application to locate transparently across the network
- Provides interaction with another application or service to be independent from network services and to be reliable, available and scaleable

Geospatial Technology and Data

Through the Office of Geographic and Information (MassGIS), the Commonwealth has created a comprehensive, statewide database of spatial information for environmental planning and management.

Mass.Gov

Mass.Gov increases public access to government services and reduces the total cost of government. In order to accomplish this, Mass.gov:

- Provides a single online face of government, a simple and consistent user interface, and organization of government services by customer need, not government structure, thereby enabling increased citizen self service and opportunities for civic engagement
- Provides a reliable 24x7 hosting platform and a suite of enterprise web publishing tools and templates that enable more cost-effective, distributed web publishing by subject matter experts
- Promotes cross-agency collaboration and compliance with standards and best practices for ensuring universal accessibility, website ease of use and increased findability

Workgroup Services

The Workgroup Services Office is committed to delivering efficient and effective services, providing solutions at highly competitive rates to our customers.
The Workgroup Office strives to continuously expand and improve its services, deliver increasing value and meet the services needs of its customers through internal and external partnerships. The Office supports a broad variety of business needs, such as running mission critical applications requiring very high availability and is comprised of the following Group:

Print & Mail Services

- Provides print and mail services for state agencies 24x7
- Ensures printing and mailing is accomplished in most cost efficient manner

1.7 Program Management Office

The mission of the **Program Management Office** (PMO) is to ensure that the Commonwealth receives full value on its capital investments in information technology. In order to accomplish this, the Program Management Office:

- Manages the Commonwealth's IT Capital Program to fund projects across state government to upgrade mission-critical systems; promote systems that can be shared by multiple agencies and provide shared infrastructure and services
- Provides project oversight services to help capital projects stay on-track and achieve business and technical needs

1.8 The Service Management Office

The **Service Management Office** (SMO) provides processes, tools and resources that enable the operation and delivery of high quality IT Services to Executive, Legislative and Judicial Branch agencies and users. As such, the SMO focuses on the framework to deliver IT Services and on strengthening the relationships with agencies and understanding information technology's contribution to their business. The following Teams make up the Service Management Office (Please click on a Team name to view a detailed org chart):

IT Service Management Team

The Service Management Team consists of The Technical Assistance Center (TAC), which ensures the health and welfare of the (Magnet) core networking infrastructure; Asset management and the Enterprise Operations Team (described below).

Enterprise Operations

The mission of Enterprise Operations is to provide IT operational support for all of ITD's customers. In order to accomplish this, the Enterprise Operations Team:

- Manages the operation and monitoring of information systems and batch processing (24 x 7) of all hosted infrastructure
- Provides IT Service Management (ITSM) services through our CommonHelp Service Desk that ensures that all service calls and inquiries to ITD are tracked from registration to closure within agreed service levels and that all requests and changes follow agreed control procedures
- Provides pro-active problem management and availability management services to increase the Mean Time Between Failures (MTBF) and reduce the Mean Time to Resolution (MTTR) of incidents.

Service Account Management

The Service Account Management Team is responsible for developing and managing the overall business relationship between the Information Technology Division (ITD) and its customers through proactive and collaborative account management. In order to accomplish this, the Service Account Management Team:

- Understands customers' business and technology needs and properly identifying and communicating their requirements, both internally and externally, while assisting and delivering successful solutions

- Ensures clear communication directly with customers regarding ITD's policies, guidelines, services, support and associated chargeback costs
- Supports ITD's Capital Plan and coordinates the Investment Brief Process

Project Management Office (MITC)

The mission of the Project Management Office MITC is to enhance ITD's ability to successfully deliver high quality projects. In order to accomplish this, the Project Management Office MITC:

- Institutes robust and consistent project management processes at ITD based on industry standards and best practices to provide accountability, transparency and predictability in project delivery
- Provides project management service for initiatives that are hosted at the ITD Data Center

1.9 Security Office

The mission of the **Security Office**, in close collaboration with the Enterprise Security Board, is to ensure the security of the Commonwealth's information technology enabled service delivery systems by constantly assessing and improving upon our cyber education & awareness, vulnerability prevention, and exploit detection & response capabilities. In order to accomplish this, the Security Office:

- Strengthens the security posture of Commonwealth information technology systems relative to their confidentiality, integrity, and availability
- Controls access to ITD managed enterprise applications (Commonwealth Information WareHouse, DocDirect, HRCMS, and VPN) as well as numerous agency mainframe applications
- Provides cybersecurity education and awareness for state and local government
- Implements and supports hardware and software infrastructure necessary to protect the Massachusetts Access to Government Network (MAGNet) community

Enterprise Security Board

The Commonwealth's Enterprise Security Board (ESB) is co-chaired by the Deputy State Auditor and ITD's Chief Security Officer, and consists of Executive, Judicial, Legislative, Constitutional Offices, Authorities, and large city/town voting members. ESB, standing committees include Strategy & Planning, Research, Education & Awareness, Variance, Standards, and Massachusetts Information Sharing & Analysis Center (MA-ISAC); members meet bi-monthly to work on enterprise security policies, standards, and related initiatives.

1.10 Technology Office

In close collaboration with the various state agencies and other ITD units, the **Technology Office** develops the architecture, standards, policies, governance, best practices and technology road map that support the business priorities of the Commonwealth. Included in the Technology Office are two of ITD's four lines of business; Network & Data Services and Hosting Services. These two lines of business are included in Engineering Services:

Engineering Services

Network & Data Services

The **Network & Data Services Office** provides core infrastructure services for customer applications and enterprise services. The Office is comprised of the following Groups:

Enterprise Communications:

- Provides Magnet Core and Wide Area Network infrastructure and support
- Offers network design and implementation services
- Provides telephony infrastructure and services for Ashburton and Saltonstall facilities
- Provides wireless device provisioning and technical support

Data Storage Management:

- Provides storage, Storage Area Network, and backup/recovery infrastructure and services for MITC Data Center
- Provides media management and disaster recovery support services

Database Management:

- Provides database systems infrastructure and systems management support
- Provides database capacity planning and systems performance management

Hosting Services

The **Hosting Services Office** provides services to state agencies who wish to host their applications services at ITD's data center located at the Massachusetts Information Technology Center (MITC) in Chelsea, MA. Currently, our services are divided among the following Groups; Unix Team, Windows Systems Services, Operating Systems, and Linux Team. These Groups provide the following:

- Choice of platforms include: IBM Mainframe zOS, Windows, AIX, HPUX, and Linux operating systems
- Operating system support consisting of system configuration, system monitoring, performance tuning, upgrade, and proactive patching
- Hardware management including break/fix as well as replacement coordination

Infrastructure Planning

The Infrastructure Planning Group provides infrastructure planning and architectural design for our new business projects and internal infrastructure initiatives. In order to accomplish this, the Infrastructure Planning Group:

- Provides infrastructure solution designs for hosting of internal and external ITD customer applications using an OSG developed infrastructure architecture framework to document, review and sign off on proposed technical architectures
- Provides enterprise capacity planning for hardware and software maintained within the Data center.

Other Technology Offices

Enterprise Policy and Architecture

The Enterprise Policy and Architecture Group is committed to providing support to customers and colleagues with an unwavering focus on ITD's values, best practices and community outreach and engagement. In order to accomplish this, the Policy and Architecture Group:

- Establishes the overall vision and strategic implementation of the SOA infrastructure
- Develops and provides oversight of cohesive Enterprise Policies, both security and non security related
- Maintains the Enterprise Technical Reference Model and Enterprise Technical Architecture which set the road map for future Enterprise Infrastructure and Operating Environments

Integration Services

The Integration Services Group is chiefly tasked with researching, developing and implementing shared oriented architecture (SOA) and SOA related technologies within the Commonwealth of Massachusetts. Current services published and supported are:

- SFED - The Secure File and E-mail Delivery Application (SFED) is a Commonwealth Shared Service available to all departments and uses a single, centralized enterprise solution to securely exchange both e-mail and files over the World Wide Web
- ePay - The ePayments component of the Massachusetts E-Government initiative is a centralized service for the Commonwealth to process electronic payments. Departmental applications that have a payment collection component can plug into a standard interface with minimal work for the business application programmer. The ePay contact is managed by the State Comptroller and ITD provides access to the Web Services portion of the ePay system
- CEO - Currently provides functionality to allow Commonwealth employees to post, approve and publish job postings and job applicants to view jobs and apply online for appropriately enabled jobs
- IT Service Management - Provides the application framework for IT Service Management processes. The mission of IT Service Management Services is to improve the customer experience with ITD. The service desk application provides a single point of contact for all customer requests that enables ITD to streamline our internal work into repeatable and sustainable processes that contribute to consistent service delivery, supports improved communications between ITD and customers which helps ITD meet customer expectations and enhances self service by providing one place to go to request services and report incidents.

1.11 ITD Employee Classifications

ITD positions fall into two categories: Bargaining Unit and Management Positions. The vast majority of state positions are Bargaining Unit positions. Bargaining Unit positions are covered by Collective Bargaining Agents (unions) who negotiate Wage and Benefit Agreements with the Commonwealth on behalf of their union members.

The National Association of Government Employees (NAGE) is the Bargaining Agent which represents ITD positions. NAGE Units 1 and 6 represent all ITD Bargaining Unit positions. Approximately one-half of ITD positions are TPL positions. The Technical

Pay Law (Chapter 717 of the Acts of 1983) went into effect at the beginning of FY85. It is designed to promote the Commonwealth's ability to recruit and retain information technology professionals by making it possible to compensate these individuals at a level more competitive with private sector standards.

Salary increases for non-TPL bargaining unit positions are negotiated by ITD and HRD and require approval by ANF..

Managers are reviewed via a process called ACES every September. Increases are approved by ANF and are based upon performance and merit.

Section 2: Federal and Commonwealth Policies

2.1 Affirmative Action, Diversity, and Equal Employment Opportunity

The Commonwealth's diversity goal is to value the differences among the Commonwealth's employees. These differences include but are not limited to race, gender, sex, color, national origin and ancestry, religion, age, mental/physical disability, sexual orientation, veteran's status, organization level, economic status, geographical origin, marital status, communication and learning styles and other characteristics and traits. This goal emphasizes the development of inclusive work environments that capitalize on each employee's skills, talents and perspectives as we set forth an unparalleled standard of excellence. It is the policy of the Commonwealth that every agency within the Executive Branch issues an Affirmative Action Plan, which describes specific objectives and actions to improve employment practices, policies, procedures and opportunities for protected group members. The Affirmative Action Plan applies to protected-group members at all levels and occupations department-wide. If you desire a copy of your agency's Affirmative Action plan, you may request a copy from your Diversity Officer. The Director of Human Resources is the Diversity Officer for ITD.

Self-Identification Process

On a periodic basis, but at least annually, the Commonwealth offers employees the option to self-identify as a racial minority, person with a disability or a Vietnam-Era Veteran for purposes of Affirmative Action status. There are two optional Affirmative Action Data Records inserts included in the employment application. The individual employee may utilize these forms to self-identify. An employee may also request the Affirmative Action Data Records from their Diversity Officer. Please note that in order to qualify for Affirmative Action status as a Vietnam-Era Veteran, the employee must apply for Eligibility Certification that is issued by the Office of Diversity and Equal Opportunity. Forms are available from the Office of Diversity and Equal Opportunity. All Affirmative Action Data Records identifying an employee as a person with a disability should be given to the agency's ADA Coordinator for handling. Should you have any questions regarding the self-identification process, please contact your agency's Diversity Officer or the Office of Diversity and Equal Opportunity in the Human Resource Department.

Veterans

Under Executive Order 478, individuals who served during the Vietnam Era are eligible to receive affirmative action protection through a certification process. The certification process is designed to ensure that Vietnam-Era Veterans and persons disabled as a result of participating in the Vietnam conflict fully participate and have equal access to employment opportunities. Certification affords the Vietnam-Era Veteran affirmative action status in hiring, promotions, demotions, transfers, and reductions in force.

Veterans must provide the Office of Diversity and Equal Opportunity with an application, which can be found on the Human Resources Division's website under Office of Diversity and Equal Opportunity and a certified copy of their Department of Defense (DD) Form 214. The form must clearly identify the type of discharge, dates of active duty, name, and social security number. Active duty does not include members of the Reserves or National Guard. The criteria by which the request for certification is verified

is: (1) a person who served on active duty for a period of more than 90 days, any part of which occurred between August 5, 1964 to May 7, 1975 and was discharged or released with other than a dishonorable discharge; or (2) was discharged or released from active duty for a service connected disability if any part of such active duty was performed between August 5, 1964 and May 7, 1975. If an application does not satisfy the established criteria, a formal rejection notification will be sent to the applicant so that the veteran may appeal the denial.

2.2 Americans with Disabilities Act (ADA)

The ADA is a federal law that prohibits discrimination on the basis of disability in employment, state and local government, public accommodations, commercial facilities, transportation and telecommunications. In the employment context, a qualified individual with a disability cannot be discriminated against in job application procedures, hiring, firing, promotion, compensation, job training, and other terms, conditions and privileges of employment. An employer has a duty, if requested, to make a reasonable accommodation to the known disability of a qualified individual if it would not impose an undue hardship on the employer's business operations.

There is also a state law protecting disabled employees from discrimination on the basis of their disability. It can be found in Massachusetts General Laws, Chapter 151B, section 4 (16). ITD's HR Director acts as the agency's Disabilities Coordinator. Please contact the HR Director if you require accommodation or further information.

2.3 Drug-Free Workplace Policy and the Governor's Annual Drug-Free Workplace Act Certification

In a good faith effort to comply with the federal Drug-Free Workplace Act of 1988, the Commonwealth seeks to ensure a safe, healthy, and productive work environment for all employees. Employees of state agencies receiving federal grant funding must accept all of the conditions required by the federal government regarding controlled substances.

In addition, both manager and bargaining unit codes of conduct specify that use of alcohol, intoxicants, narcotics, or controlled substances in any form is prohibited while on duty. Similarly, no employee shall report for work under the influence of intoxicants, narcotics or controlled substances in any form. The only exception to this rule is the use of medication when prescribed for the treatment of the employee by a registered physician or dentist.

2.4 Ethics

2.4.1 Codes of Conduct

All managers and employees covered by a Code of Conduct are required to read the Code and sign the receipt form within ten days, attesting that they have a responsibility to read and comply with the provisions of the Code. Some state departments have their own agency handbook as well that governs the behavior of their employees.

Managers and Confidential Employees

Respecting and honoring the public trust placed in those who work in state government is an issue of paramount importance. In order to ensure that you are cognizant of your obligations and have full understanding of the implications of your actions and/or

omissions, the Executive Office for Administration and Finance has issued a Code of Conduct for Managers and Non-Union employees.

The Code covers topics such as:

Conflict of interest
Outside employment and business activity
Public records
Legislative requests
Political activities
Drug and alcohol use
Weapons
Department ID cards and badges

The code may be accessed on the HRD Website:

http://www.mass.gov/Eoaf/docs/hrd/policies/files/manager_code_of_conduct.rtf

Bargaining Unit Employees

Collective bargaining contracts also contain codes of conduct similar to that of managers/confidential employees, which include additional issues that are important to individuals in these professions and have been negotiated with the unions.

The NAGE Code of Conduct is posted to the ITD Employee Portal:

http://www.mass.gov/Aitdintranet/docs/hr/bu6codeofconduct.doc

2.4.2 Campaign and Political Activity

The Campaign Finance Law (Massachusetts General Laws, Chapter 55) does not prohibit public employees from engaging in political activity, as long as such activity: 1) is not undertaken during work hours or otherwise using public resources, and 2) does not include soliciting or receiving political contributions.

The Campaign Finance Law (Massachusetts General Laws, Chapter 55) prohibits all compensated state, county, and municipal employees from:

Selling tickets to a political fundraiser or otherwise soliciting or collecting contributions in any manner, such as by phone or mail
Serving as treasurer of a political committee
Allowing the employee's name to be used in a solicitation letter or fundraising phone calls
Helping identify people to be targeted for political fundraising
Using public resources for political campaign purposes, such as influencing the nomination or election of a candidate or the passage or defeat of a ballot question

The Massachusetts conflict of interest law (MGL c. 268A) prohibits all state, county, and municipal public employees, whether compensated or not, from:

Using any public resources or facilities, or the state seal or coat of arms, for campaign purposes.
Engaging in any campaign activities during their normal public working hours

(For appointed employees) Soliciting campaign contributions or services, or anything else of substantial value, from subordinate employees, vendors they oversee, or anyone within their regulatory jurisdiction

Representing a campaign (or anyone else) in connection with some matter in which the employee's own level of government (state or local) has a direct and substantial interest (unless they are "special" employees)

For more information, contact the Office of Campaign and Political Finance or the State Ethics Commission or ITD's legal counsel or refer to these web sites:
http://mass.gov/ocpf

http://www.mass.gov/ethics

2.4.3 Conflict of Interest and Financial Disclosure Policy

Chapter 268A of the Massachusetts General Laws requires that state employees give undivided loyalty to the state and act in the public interest rather than for private gain. This law sets forth a minimum standard of ethical conduct for all state employees and officials. The purpose of the law is to ensure that public employees' private financial interests and personal relationships do not conflict with their public obligations. The law governs what you may do on the job, what you may do after hours or "on the side," and what you may do after you leave public service. It also sets standards of conduct for all state employees and officials. The State Ethics Commission provides free, confidential legal advice about how the law applies in a particular situation. We encourage you to seek legal advice from the Commission or your agency's legal counsel if you face a potential conflict of interest.

All state employees are encouraged to complete an online training program on state ethics.

Some employees may be required to file annual financial disclosure forms with the State Ethics Commission.

For more information on on-line training or financial disclosures, contact the Massachusetts State Ethics Commission or refer to this web site:
http://www.mass.gov/ethics

2.4.4 Negotiating Employment Information

The State Ethics Commission has published an advisory with guidelines for state employees who are contemplating or commencing negotiations for prospective employment. You can find the full text of Advisory Number 90-01 on the State Ethics Commission website – http://www.mass.gov/ethics - using the search term "negotiating employment".

2.5 Sunshine Policy

Executive Order 444, section 1 states that, "Each person applying for employment within the Executive Branch under the Governor must disclose in writing, upon such application, the names of all immediate family as well as persons related to immediate family by marriage who serve as employees or elected officials of the Commonwealth." In this policy, immediate family member is defined as spouse, child, parent, and sibling and those related to individuals by marriage (i.e. the spouse's child, parent, and sibling.)

Section 3: General Employee Information

3.1 Attendance and Hours of Work

You are responsible for arriving at and leaving work at the times agreed upon in the work week schedule authorized by your supervisor, including returning on time from all break periods. If you are unable to report to work, notify your supervisor at the beginning of your usual workday, or as soon as possible. Be sure you understand your work schedule and ask your supervisor if you have questions. If you are absent from work without authorization from your supervisor, you may be subjected to disciplinary action, up to and including discharge from state service.

Unless otherwise specified, standard work hours are 8:45 am – 5:00 pm with a 30 minute unpaid lunch break and one fifteen minute paid break.. You cannot charge your 1/2-hour lunch period toward your obligation of a 37.5-hour workweek. Employees are required to take a 30 minute unpaid break for each shift they work longer than six hours. This standard applies to managers and NAGE employees to ensure standardized compliance with "Rules Governing Paid Leave And Other Benefits For Managers And Confidential Employees" (the "Redbook"), applicable collective bargaining agreements, and MGL 149, section 100.

3.1.1 Recording Time

Each week, every ITD employee must report a full week's time in Clarity. This would include all project work as well as any payroll exceptions. All time must be reported by day.

- Total weekly time reported must be equal to or greater than the employee's calendar time. For example, if you work a 37.5 hour week, you must post at least 37.5 hours in your timesheet in Clarity.
- All time must be reported and submitted by employees no later than 10:00 am on Friday of each week. Anyone not working on Friday is responsible for completing their time reporting before they leave for the week.
- Timesheet approvers should review and approve timesheets no later than 12:00 noon on Friday.

Weekend Changes: If you work over the weekend, either by regular schedule, changes in planned overtime, or callback:

- You should notify your supervisor on Monday.
- Your supervisor should then return your timesheet to you for edits.
- You should correct your timesheet to reflect hours actually worked and submit to your supervisor for approval.
- Your supervisor should then approve your edited timesheet and notify LaRoyce Jacks and Patricia Keddy that a change is needed in HRCMS.

Please review your collective bargaining agreement or the "Rules Governing Paid Leave and Other Benefits for Managers and Confidential Employees", available on the Human Resource Division website:

http://www.hrd.state.ma.us/agency_services/AS_Manage_Workforce/rulesandguidelines.htm

3.1.2 Flexible Work Arrangements

Some departments/managers in ITD may offer flexible work schedules including part-time work and job sharing. Flexible work schedules must be approved by your manager and Human Resources in writing. ITD retains the right to revert to a standard 5 day 7.5 or 8 hour work schedule at any time, as long as the employee is given two weeks notice per BU rules. Request for flexible work schedules must be submitted in writing to your supervisor and must include justification, duration, and purpose. Flexible work schedules are at the manager's discretion and can be changed at any time due to business/departmental needs.

*See Telecommuting Policy in Appendix F

3.2 Collective Bargaining Agreements

Collective bargaining governs the Commonwealth's work force along with the civil service/merit system. The statutory framework for collective bargaining for state employees is contained in Chapter 150E of the General Laws, which was enacted in 1973. Chapter 150E extends to all employees the right to organize and bargain collectively over wages, hours, and other terms and conditions of employment, except for the following:

Managerial employees are excluded from the coverage of the Law because they formulate policy. Their job group (i.e., M I-XII) can generally identify such persons.

Confidential employees are excluded because they directly assist and act in a confidential capacity to a managerial employee who may be in a policy-making/labor relations position (e.g., secretary to an agency head). No employee is considered to be confidential unless approved by the Human Resource Division.

Currently, all bargaining units are covered by collective bargaining agreements. These agreements generally continue in effect until a successor agreement is negotiated. The agreements determine the wages, hours, and benefits in the units covered by the agreements. The agreements are binding on all state managers and supervisors who supervise bargaining unit employees and cover a wide range of topics, including:

compensation
criteria and procedures for provisional promotion
regulation of leave benefits
procedures for transfers and shift and day off selection
work schedules, overtime, and compensatory time
holidays
health insurance contributions
affirmative action/non-discrimination
layoff procedures
disciplinary procedures

For more information about collective bargaining, please contact your union representative.

See M.G.L. Chapter 150E

Bargaining Unit Positions

Bargaining Unit positions, and the employees who occupy them (regardless of the funding source), are covered by Collective Bargaining Agents (unions) which negotiate Wage and Benefits Agreements with the Commonwealth on behalf of their union members and those employees occupying the positions under their authority and represent employees with regard to labor relations activities, as appropriate. Upon appointment to a Bargaining Unit position, employees automatically receive the benefits and coverage of the current applicable Bargaining Unit Agreement, with the exception that, during the six-month probationary period, grievance and arbitration rights do not apply in the event of disciplinary action or termination of employment.

The National Association of Government Employees (NAGE) is the Bargaining Agent that covers funded Bargaining Unit positions at ITD. An Employee Obligation clause is contained in all Bargaining Unit Agreements requiring that, as condition of employment, an employee occupying a Bargaining Unit position is obligated to join the union and consent to the weekly deduction of Union Dues from the employee's pay check, or, if the employee elects not to join the union, authorize the weekly deduction of an Agency Fee from the employee's pay check. Either form of deduction is paid to the Bargaining Unit. It is the employee's obligation to contact the Union in order to authorize the deduction of either Union Dues or the Agency Fee. The Bargaining Unit has the right to request the removal of any employee who is occupying a Bargaining Unit position who is not a dues-paying member of the union, or is not authorizing the deduction of the Agency Fee.

Union members are able to participate in union activities, vote in union elections and vote for the ratification of proposed negotiated contracts. Employees who elect to pay the Agency Fee receive all benefits contained in applicable Wage and Benefits Contract Agreements, but are not eligible to participate in union activities, vote in union elections or for the ratification of proposed contracts.

Union Dues for full-time NAGE Unit 1 employees are currently $ 23.30 bi-weekly.

Union Dues for full-time NAGE Unit 6 employees are currently $23.50 bi- weekly.

Agency Fee for full-time NAGE Unit 1 employees is currently $22.70 biweekly.

Agency Fee for full-time NAGE unit 6 employees is currently $22.90 bi- weekly.

Union Dues for part-time NAGE Units 1 and 6 employees are currently $15.70 bi-weekly.

Agency Fee for part-time NAGE Units 1 and 6 employees is currently $15.50 bi-weekly.

In addition to your union dues or fees, you may or may not choose to have an additional $1.00 bi-weekly deducted for a political education fund (called COPE) that is administered by the union.

NAGE is located at 159 Burgin Parkway, Quincy, MA, 02169 (Telephone 617-376-0220).

3.3 Courtesy

You are expected to conduct yourself courteously and responsibly at all times. Remember that the image of your organization rests upon the behavior of the employees who represent it. You represent the Commonwealth of Massachusetts and it is important for you to make a positive impression for those you serve, the citizens of the Commonwealth, as well as your colleagues.

Every ITD employee has an obligation to demonstrate professionalism at all times and conduct themselves at all times with the public and their colleagues in a courteous and professional manner.

3.4 Disciplinary Action

The Information Technology Division may use disciplinary action to correct the conduct of an employee.

Violations of ITD or Statewide policies may result in disciplinary action. Some of the violations that can result in disciplinary action include:

failure to perform assigned responsibilities

active disruption

abusive or violent behavior

chronic absenteeism

tardiness

refusal to carry out direct requests or instructions

incompetence

Disciplinary Procedures

Several essential elements must be present to affirm disciplinary action: sufficient cause/repeated inappropriate behavior such as tardiness, absenteeism, or substandard performance. Such cause is established by (1) building a record of employee's knowledge of behavior and performance expected of them, (2) consistently administering the standard, (3) providing clear, documented warnings that state the exact type of inappropriate behavior and a satisfactory length of time for the employee to improve their conduct or work performance.

Warnings fall in two categories:

Informal verbal warnings: given by the supervisor during a structured conversation at a time and place set aside from the regular work site with employee feedback. Documentation of warnings of this type will be placed in the employee's personnel file.

Formal written warnings: a letter handed to, and consequently signed by the employee stating a period of time during which the employee must improve or cease the undesired behavior as requested during prior verbal warnings.

The initial discipline must be related to the severity of the act, and then more severe penalties should be administered for each additional offense. If, after warnings and disciplinary actions, an employee's conduct does not improve, termination may result.

Bargaining Unit employees are entitled to request union representation under 'Weingarten Rights'. http://www.nage.org/state/work_rights.shtml

Employee Appeal Procedures

After completing the contractual probationary period, disciplinary action may be appealed under the grievance arbitration procedures of the applicable Collective Bargaining Agreement. An employee may appeal if s/he can establish that the discipline was motivated by improper factors such as age, race, sex, union activity, and mental or physical handicap. Employees may appeal to the Massachusetts Commission Against Discrimination, the Equal Opportunity Commission, or the Labor Relations Commission.

3.5 Dress Code

ITD is a professional organization in the business of customer service. The impression we make on our customers is critical to the success of our business. A very large part of the impression we make as individuals and as a business is reflected in our appearance. It is recommended that ITD employees adhere to a policy of business or business casual dress.

3.6 Expectation of Privacy

Any documentary materials or data made or received by an employee of the Commonwealth, regardless of their physical form, may be considered a public record subject to the Public Records Law. To find out more about the Massachusetts Public Records Law, please refer to http://www.sec.state.ma.us/pre/preidx.htm or Massachusetts General Laws, Chapter 4, Section 7(26).

In addition, you should be aware that objects and areas in which you may keep personal belongings, including but not limited to desks, filing cabinets, email and voicemail mailboxes, the hard drives of all IT devices, and lockers, are the property of the Commonwealth and may be accessed by your employer at any time. ITD employees should have no expectation of privacy regarding their workspace or their use of the Commonwealth's information technology resources.

3.7 Guidelines for Managing Contractors

There are basically two reasons to hire a contractor. The most common reason is that the organization doesn't have the expertise in-house to complete a task or project with specific scope and deadlines; the other is the contractor is hired as an 'extra hand' for a specific period of time. While IT contractors provide a valuable service to the organization, it is critical that managers clearly distinguish the difference between managing the work done by a contractor and the work done by a state employee.

The Hiring Manager is responsible for adhering to the following guidelines:

- **Develop and maintain specific goals and schedules.** The more direction you can give a contractor, the more likely you will be to achieve your management goals. Document clear and specific goals, and provide time frames for projects that include interim check-ins.
- **Contractors are paid only for hours worked**. Managers should be vigilant in ensuring that contractors are paid only for hours worked. Managers should set specific work schedules and ensure the contractor adheres to the schedule.

Contractors should not be paid for: lunch; break periods; sick time; vacation time; snow days or early release days. The Commonwealth is legally bound to paying contractors only for actual hours worked.

- **Contractors cannot bill more than 37.5 hours per week (and no more than 48 weeks per year) without prior approval of TFG and HR Governance Board**. ITD is responsible for complying with overtime provisions of the Fair Labor Standards Act. ITD assumes full liability if violation occurs.
- **Contractors need to be able to fully document tasks and deliverables each week.** Managers should meet with contractors weekly (preferably Friday) to review the previous week's tasks and deliverables. At the end of this meeting the manager can review and approve the contractor's time sheet. A contractor's time sheet can only be approved by the person providing direct, daily supervision.
- **Contractors must clearly document tasks in Clarity every week.** Managers are responsible for ensuring that hours approved in Clarity match the invoice received from vendor. Managers must also check the monthly update distributed by TFG which outlines hours encumbered and hours used on contracts.
- **Contractors cannot supervise state employees.** A contractor may provide guidance to state employees on tasks but cannot supervise or evaluate the work of employees.
- **Managers need to be able to identify when contract will terminate.** A contractor should be working for a limited purpose and a finite period of time.
- **Contractors should consistently provide the highest level of performance.** If at any time the manager does not feel that the contractor is performing at the highest level, the manager should contact the vendor and terminate contract immediately. Neither contractor nor vendor should ever receive severance pay. Contractor is only to be paid for hours worked.
- **Contractors must acknowledge receipt of and comply with ITD's Acceptable Use Policy; Confidentiality; Workplace Violence; and Sexual Harrassment policies.** Any product produced by the contractor is the property of the Commonwealth.
- **Contractors must acknowledge receipt of (in writing) 'Representations by Resources' as outlined in ITS33.**
- **Carefully integrate your contractors**. Clearly, full- and part-time employees enjoy different benefits than contractors. Still, people's hiring status should not divide the office. In other words, make sure all your workers know that they are valued contributors on one team. Integrate them functionally when you need to. Use caution, however, when including contractors at company events. You don't want to create a situation in which the contractor's status begins to move toward that of an employee. A contractor should not be billing time spent at company events and should only attend 'all staff' events if germane to their work**.**
- **Reassess the contractor's status after 6 months** to determine either prospective end date or the creation of a full time position. Only specific project based contracts should last more than 12 months.
- **Manager should never negotiate or discuss terms of the contract with the contractor**. Any discussion of contract terms (including rate changes) is strictly with the vendor who is the contractor's employer. If approached by contractor with request for contract changes tell contractor that you can only deal with the vendor.

3.8 Health and Safety in the Workplace

3.8.1 Medical Emergency Procedures

McCormack Building

In the event of a medical emergency in the McCormack Building/One Ashburton Place, activate one of the three procedures listed below depending on the emergency. Be prepared to give the floor, room number (if available), tenant, and type of medical emergency if known. If possible have the name, age, and date of birth of the patient written on a piece of paper and available to the first emergency responder.

Call BSB Control Center at (617) 727-1000. This line is staffed 24x7 and will co-ordinate the notification of 911 emergency services and State Police as necessary.

If it is imperative to call 911 directly, you can reach the 911 service from ITD phones by dialing 9911. After calling 9911, please notify the BSB Control Center immediately and inform them that a 911 call has been placed. Supply the BSB Control Center with the same information given to the 911 operators.

Call the Mass State Police in the McCormack Lobby by calling (617) 727-2917. Please notify the BSB Control Center immediately and inform them that a call to the State Police has been placed. Supply the BSB Control Center with the same information given to the State Police.

MITC

In the event of a medical emergency in the MITC/200 Arlington Street Chelsea location,, activate one of the two procedures listed below depending on the emergency. Be prepared to give the floor, room number (if available), tenant, and type of medical emergency if known. If possible have the name, age, and date of birth of the patient written on a piece of paper and available to the first emergency responder.

Call Lincoln Properties Building Security Control Center at (617) 660-5555. This line is staffed 24x7 and will co-ordinate the notification of 911 emergency services and State Police as necessary.

If it is imperative to call 911 directly, you can reach the 911 service from ITD phones by dialing 9911. After calling 9911, please notify the Lincoln Properties Control Center immediately and inform them that a 911 call has been placed. Supply the Lincoln Properties Control Center with the same information given to the 911 operators.

Notify Employee's Emergency Contact

Emergency Contact Sheets are maintained for all ITD staff by the Human Resource Unit. The employee experiencing the medical issue should be consulted for information on who to contact on their behalf. If the employee is unable to give instructions, their supervisor or manager should contact HR for assistance in notifying the individual's "emergency contact".

Notify Worker's Comp Representative

Once the emergency response has been activated, please immediately notify the ITD Worker's Compensation representative, LaRoyce Jacks, at (617) 626-4418.

3.9 Investigations of Workplace Misconduct

Any allegations or reports of potential workplace misconduct, especially those specifically related to possible policy violations, may be subject to investigation by a member of the Human Resources team or their designee. Investigations are initiated so that ITD as an organization can insure consistent standards for policy compliance and expectations for how people behave in the workplace are clearly and consistently communicated.

All investigations are guided by the following principles:

- Interviews are conducted with all individuals who have first hand knowledge of the incident to gather facts and data so that a response will be based on the actual events and not past history or opinions or hearsay.
- Confidentiality will be maintained to the greatest degree practical limited only by requirement for Human Resources to respond to the information gathered
- Retaliation for participating in an investigation is not tolerated

3.10 Leaving State Service

3.10.1 COBRA Medical Coverage

Consolidated Omnibus Budget Reconciliation Act of 1986 (COBRA) Under Title X of a federal law commonly known as COBRA, certain former employees, retirees, spouses, former spouses and dependent children have the right to temporarily continue their existing group health coverage at group rates when group coverage ends as the result of certain employment or life events. The cost for COBRA coverage is 102% of the full cost group premium. The GIC administers COBRA coverage.

Leaving State Service and GIC Life and Health Benefits

Leaving State Service with Fewer Than 10 Years of Full-Time Service

If you are leaving state service but have fewer than 10 years of full-time service (as determined by the State Board of Retirement), you may continue your health insurance coverage with the GIC for any reason other than termination for gross misconduct and with some limitations on time and/or benefit levels in one of the following ways:

COBRA - health only (you have 60 days to elect COBRA coverage, but the coverage begins the first day of the month following the coverage end date. To avoid owing retroactive premiums, send in your COBRA application promptly to the GIC):

Benefit: Allows you to stay in the same plan with the same group benefit.

Drawbacks: You pay 100% of the premium, plus 2% for administration (no Commonwealth contribution). Maximum duration of coverage is 18 months.

Convert to Non-Group health coverage with your current Plan:

Benefit: Can keep coverage beyond 18 months.

Drawback: Benefits are almost always less comprehensive than GIC coverage.

Life Insurance Portability - Continue your amount of basic life and optional life coverage with some limitations:

Benefit: Continue term life coverage at a competitive rate.

Drawback: Does not include health coverage.

Convert to Non-Group life coverage with the current carrier:

Benefit: Ability to continue life insurance coverage.

Drawback: Benefits almost always less than GIC plan coverage.

Leaving State Service With 10 or More Years of Full-Time Service

If you are leaving state service with 10 or more years of full-time service (as determined by the State Board of Retirement) you may be eligible for a state pension. If you choose to collect your state pension at a later date, the GIC recommends that you elect Deferred Retirement coverage. If you are getting health coverage elsewhere, the GIC suggests that you keep, at a minimum, basic life insurance, paying 100% of the premium. At retirement, you may resume GIC health coverage; the Commonwealth will contribute the prevailing contribution percentage for retirees. If you are not getting health coverage elsewhere, keep your GIC basic life and health insurance, paying 100% of the premiums until retirement.

If you decide not to leave your money in your retirement system, your benefits as a Deferred Retiree end. You may elect to continue your health and life coverage, with some limitations on time and/or benefit levels, in one of the following ways: GIC COBRA health coverage only, conversion to Non-Group health coverage with current carrier, portability of life insurance, or conversion to non-group life insurance with current carrier.

Keeping Your Address Current

If your mailing address should change once you leave state service, it is important to notify, in writing, particular agencies of the change. You need to notify: 1) the State Board of Retirement, 2) the Group Insurance Commission, and 3) your prior Department. This is to ensure that W-2s, retro pay, etc. are mailed to your correct address.

3.10.2 Resignation Notice

If you are resigning, please present your supervisor and/or manager with a minimum written two weeks notice of such action. At a minimum, your resignation notice should include the date of your last day of work and a mailing address.

3.10.3 Retirement

You are vested in the state retirement system once you have accumulated the equivalent of 10 years of full-time service.

If you leave state service you may 1) receive a refund of your retirement contributions, with 20% deducted for federal taxes or 2) roll it over into a tax-qualified vehicle. Under certain circumstances, there may be a penalty for early withdrawal.

If you leave state service after you are vested and before you are old enough to retire you may leave your retirement contributions in the system and receive a state pension at age 55.

Retirement and GIC Changes

See the GIC's website or the GIC's Retiree/Survivor Benefit Decision Guide for health and life coverage options at retirement.

Unemployment Insurance

The Commonwealth contributes towards the unemployment insurance system on your behalf. In the event you are separated from your position, you may file a claim with the Division of Unemployment Assistance (DUA). The Commonwealth will verify the reasons for your separation and the DUA will determine eligibility.

3.11 Parking

Parking spots at One Ashburton Place are allocated by the Bureau of State Office Buildings. Each agency is allotted a discreet amount of spaces. The agency head determines the allocation of parking spots. ITD's parking passes are designated to members of the Executive Staff and those who require 24/7 access to the building for technology and operational needs. The Bureau of State Office Buildings is solely responsible for the allocation of parking spaces for individuals who may require parking due to medical needs.

Parking spots at MITC are allocated by Lincoln Properties. Each agency in the building is allotted a discreet amount of spaces. The agency head determines the allocation of parking spots within ITD. Specially designated handicapped parking spaces are available in Lot A on the south side of the building. In addition, handicapped parking is available for MITC visitors in the Visitor's Lot. Lincoln Properties is solely responsible for the allocation of handicapped parking spaces.

3.12 Performance Appraisals

Your job performance will be evaluated twice annually. You and your supervisor will participate in the regular employee appraisal process throughout your career. This gives you and your supervisor an opportunity to discuss your job performance and career development. There are two systems for Performance Evaluation. The evaluation system for employees in Management positions is called Achievement and Competency Enhancement System (ACES). The evaluation system for all bargaining unit employees is called the Employees Performance Review System (EPRS).

The Human Resources Division publishes extensive information on ACES and EPRS. This information is accessible on their website, www.mass.gov/hrd, click on "State Employee Benefits and Compensation", then click on "Performance Reviews & Management Compensation".

3.13 Performance Recognition Program

The Commonwealth's Performance Recognition Program gives formal recognition to employees who make meaningful contributions which distinguish them from their peers. These special awards focus attention on consistent, positive achievements by both individuals and teams of state employees, and recognize those who demonstrate innovation and dedication to their work, concern for the public trust, and a commitment to excellence.

3.13.1 Kudos

ITD encourages all employees to embody the ITD values. Any ITD employee or manager who believes a co-worker or team at ITD has been clearly displaying examples of ITD values is encouraged to submit kudos to be published to the ITD employee web portal. Kudos can be submitted based on personal observation, or in response to input from a customer that an employee or team has gone above and beyond their duties to meet customer needs. Kudos can be submitted via email to any member of the Human Resource team for publication to the employee portal. Publication is made to www.mass.gov/itdemployee, under "Forms & Publications".

3.14 Personnel Files

You have the right, upon request, to examine and receive copies of any and all materials contained in your official Personnel File relating to your employment. Please allow a reasonable amount of time for a file to be copied.

3.15 Probationary Period

In order to determine if you can successfully perform all of the duties of your position, you will serve a probationary period. The length of your probation depends on your particular job, but it is generally six months in duration. Your job description/duty statement describes your responsibilities and the standards for accomplishing the specific tasks or set of duties.

If you are an employee covered by a collective bargaining agreement, you may request union representation during disciplinary proceedings during the probationary period, but you do not have rights to appeal disciplinary action taken against you during this time.

ITD employees in their probationary period are not eligible for promotion or transfer to different positions within ITD. Employees may be considered for promotion and transfer upon successful completion of their probationary period.

3.16 Protection of Sensitive Agency Information

Commonwealth government organizations have a duty to ensure that personal information collected, used, maintained, or disseminated in the process of providing services to the public must be safeguarded against loss or theft. To that end, it is essential for all Commonwealth departments and agencies to ensure that sensitive information, in particular personal information, is protected.

A definition of highly sensitive information is provided in the Commonwealth Enterprise Information Security Standards for Data Classification Version 1.0, published October 26, 2007
(http://www.mass.gov/Eoaf/docs/itd/policies_standards/DCStandardsDraftFD.rtf)

as follows:

- High Sensitivity data may include, but is not limited to, personally identifiable, legally mandated, or sensitive data associated with: investigations, bids prior to award, personnel files, trade secrets, appraisals of real property, test questions and answers, constituent records, health records, academic records, contracts during negotiation and risk or vulnerability assessments.

All ITD Employees are responsible for ensuring that sensitive information, in particular personal information, is protected by adhering to the ANF Acceptable Use Policy and the terms of the Information Technology User Responsibility Agreement. In addition, users will see the following prompt each time they login to the ITD LAN.

ITD Employees and Contractors (All Users)

"In the course of performing their jobs, Agency employees and contractors often have access to confidential, [sensitive] or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations." http://www.mass.gov/Eoaf/docs/itd/policies_standards/acceptableuse.pdf

Under no circumstances is it permissible for employees or contractors to acquire access to confidential data unless such access is required by their jobs.

1. Under no circumstances may employees or contractors disseminate any confidential information that they have rightful access to, unless such dissemination is required by their jobs.
2. Under no circumstances may employees or contractors save any confidential information to a local hard drive and/or removable drive (e.g., C drive of laptops or employee's personally owned PCs, thumb- or jump-drives, communication devices, CDs or sent as an attachment to an email message., etc.), unless required by their jobs.
3. Under no circumstances may employees or contractors remove any confidential information, unless such removal is required by their jobs.
4. Sensitive information should only be stored on password protected network drives or encrypted files.

Privileged Users

Due to the nature of the work ITD performs, many users of ITD is information technology resources have a higher level of access to computer systems than simple use of application functionality. These users are defined as "privileged" users. "In computing, privilege is defined as the delegation of authority over a computer system. A privilege in is a permission to perform an action[1]"

Principle of Least Privilege

"In information security, computer science, and other fields, the **principle of least privilege**, [also known as the **principle of least authority**] requires that in a particular abstraction layer of a computing environment every module (such as a process, a user or a program on the basis of the layer we are considering) must be able to access only such information and resources that are necessary to its legitimate purpose.[1][2]"

Conformance to the principle of least privilege protects users and ITD from misuse or compromise of access granted to users. All ITD staff, privileged users or not, must be aware of Enterprise Information Technology policies and comply as applicable.

3.17 Provisioning New Employees

New employees are provisioned with basic tools for completing their work through the ITD work management system. The hiring manager, or designee, is responsible for opening the service request in the work management tool. Detailed instructions for completing the process are posted to the ITD employee portal.

3.18 Public Records Requests and Talking with the Media

All public records requests must be forwarded to the ITD General Counsel for response. The making of such a request creates legal rights and responsibilities that ITD must consider in making a response. This issue is particularly sensitive at ITD because we hold information for many other agencies, in addition to information technology security information. A public records request occurs any time someone outside the Executive Department requests a copy of a record from ITD. Although record requests made by Executive Department employees may also raise legal issues if the documents requested involve confidential material, they need not be treated as public records requests.

The requestor does not have to use the words "public records request" or "freedom of information act" in order to have their request treated as a public records request. Nor do they have to put their request in writing. For example, a disgruntled vendor who lost out on an ITD contract for which they had bid makes a public records request when he calls up the ITD employee managing the procurement and asks for copies of all of the bids submitted by other vendors.

While contractors, like other third parties, have the right to access public records, you do not have to treat as a public records request a contractor's request for a Commonwealth document necessary for the performance of the contractor's contract. If you are working with a contractor on a development project and they ask for documentation for software

[1] http://en.wikipedia.org/wiki/Privilege_(computer_science)

ITD already owns that is relevant to the development project. you don't have to treat his request as a formal request and you can simply turn the document over. In cases where a requested document contains data that can not be disseminated due to legal or policy restrictions, contact the General Counsel.

In the past, a record was a piece of paper bearing some information. Today, ITD holds relatively few paper documents, and many types of electronic documents. The courts interpreting the public records law treat electronic documents as the equivalent of paper records. Web pages, data stored on servers, backup tapes, and videotapes are all "records" under the public records law. ITD may on some occasions be required to extract data from a database for the purpose of responding to a public records request, but is not required to write code to achieve such a goal.

The public records law, as interpreted by the Secretary of the Commonwealth, does not permit ITD to make any inquiry about the purpose to which the record sought will be put, or to consider the requestor's purpose in making a determination as to whether to turn over the document or not. At the same time, if dissemination of public record would endanger individuals or groups of individuals, the General Counsel will consider refusing the request and letting the requestor appeal up to the Secretary and the court.

The Secretary of the Commonwealth has posted a guide to the public records law at http://www.sec.state.ma.us/pre/prepdf/pubreclaw.pdf

3.19 Solicitation of Charitable Donations in the Workplace

ITD resources including email and photocopy machines should not be used by to solicit charitable donations within the workplace, with the exception of the COMECC Campaign. Employees may approach co-workers for support of charitable causes, provided they are not in violation of the conflict of interest law, codes of conduct or any other existing policies or procedures. Anyone seeking donations from co-workers for a charitable cause should take care not to exert undue pressure on co-workers or supervisees to make donations or contributions of any kind.

3.20 Staffing and Notification Procedures for Emergency Situations

These procedures are designed to allow the unhindered operation of the critical systems and applications the Information Technology Division supports so that all clients and persons entrusted to the care and custody of the Commonwealth will continue to receive necessary services. Compliance with these procedures is intended to ensure that the Information Technology Division can serve the needs of its customers and the public at large while still ensuring the safety and well being of its employees.

Emergency Personnel:

ITD has identified Emergency Personnel who may be required to report to their assigned work site as scheduled, regardless of an emergency situation, due to the critical nature of their job functions and requirement that they be on-site to effectively serve their function.

Notification to Senior Management:

If the Governor makes a decision that would impact the staffing of state offices during an emergency, MEMA will contact HRD who will be responsible for contacting each Cabinet Secretary and Division Director regarding the decision of the Governor.

(MEMA will assume this responsibility if HRD is unable, due to the emergency, to carry out this function.) Each Secretariat and Division Director is charged with ensuring that this decision is communicated throughout their Secretariat/Division utilizing its pre-established Employee Notification Plan.

In addition, official information regarding the emergency situation will be posted on the Commonwealth's website: www.mass.gov. In addition to the website, MEMA will help facilitate communication by publicizing any decision regarding the staffing of state offices on television and radio news channels, as a part of school and other community cancellations.

Employee Notification Process:

In order to be prepared for an emergency or early release of personnel, ITD has prepared an Emergency Personnel List containing the following information: the position title and functional title of all Emergency Personnel, and delivered written notification to all employees designated as Emergency Personnel. Supervisors and Managers of Emergency Personnel are responsible for coordinating communications regarding shift coverage during emergencies.

Non-Emergency Personnel are informed that they do not need to report to work via declaration of emergency as posted to www.Mass.gov homepage and/or email from ITD Director of Human Resources. Supervisors and Managers of staff are responsible for communication with team members to assure adequate coverage of team duties and/or reassessing business priorities in response to the emergency. All means of communicating should be considered, including websites, voicemail messages, group e-mails, and phone trees.

Impact on Non-Emergency Employees

The emergency situation could impact Non-Emergency Personnel in two ways:

The first situation is where employees are informed that, for the purposes of restricting vehicle movement throughout the state or specific counties/municipalities, only Emergency Personnel need report to work. (However, if the Appointing Authority determines that it is safe to do so, it may permit access for Non-Emergency Personnel who wish to report to work.)

The second condition is where Non-Emergency Personnel are either permitted to be released early or to have a delayed arrival time. Such directive may apply either statewide or to a specific area of the state. All employees designated as Emergency Personnel will be expected to be at their posts until properly relieved. In any case, Appointing Authorities are not to release any employees until directed to do so by the procedures outlined in this document, even if an individual municipality establishes a local State of Emergency.

Non-Emergency Situations:

There may be an occasion that, although not considered an emergency situation, creates an intolerable working situation for employees. Examples may include the lack of water, electricity or heat in a state-owned or leased building. In these instances, before employees are permitted to leave early, clearance must be obtained through the agency's

Secretariat or Division Director. In order to ensure consistency, however, the Secretariat or Division Director must consult with the Chief Human Resources Officer before taking such action.

Leave Benefits:

Employees who had requested and were approved to use paid leave (e.g., Vacation Leave, Personal Leave, Sick Leave, or Compensatory Time) on a day, or any part of a day, in which a State of Emergency is declared or an employee release directive is issued, shall be charged with that paid leave as previously requested and approved. Employees who work or remain at work under such conditions are not entitled to compensatory time or any other compensation. Time-off provided to Non-Emergency Personnel as the result of an emergency situation will not be considered a leave benefit.

Section 4: Payroll Information

If you have any questions on any items in this section, please contact your Payroll and Benefits Manager.

4.1 Bi-Weekly Pay

The Commonwealth uses a bi-weekly (14 day) payroll system. Payroll schedule is every other Friday. Payroll Schedule can be found at: http://www.hrcms.state.ma.us/

All employees are required to have direct deposit for your bi-weekly pay. ITD uses PayInfo, a web-based tool, for employees to access payroll information. PayInfo is accessible using a PC with an internet connection 24 hours a day, 7 days a week. Each payday your PayInfo will be updated to include: gross bi-weekly itemized earnings; year-to-date gross earnings; net earnings; the type and amount of deduction; sick, vacation, personal leave and compensatory time balances.

Please review your payroll advice each pay period to ensure the accuracy of the information contained, since corrections may be prohibited after a period of time elapses. Please immediately notify your Payroll Manager or Human Resources Director of any issues you have with the accuracy of your pay advice.

4.2 PayInfo: Electronic Paystub/Pay Advice Distribution

Paystubs, also referred to as Pay Advices, are distributed electronically through the "Payinfo" system. The Office of the State Comptroller publishes an informational brochure on the PayInfo system which can be accessed using the following link:

http://www.mass.gov/Aosc/docs/business_functions/bf_payroll_lcm/PayInfo2008.pdf

You can login to the system directly using the link below:

https://payinfo.state.ma.us/payinfo/Login.asp

If you need further assistance, please contact your payroll administrator.

4.3 Employee Expenses and Travel Reimbursements

Generally, if you are approved to use your personal automobile for work-related travel, you will be reimbursed for mileage. This mileage reimbursement is intended to cover your cost of garage fees, parking, tolls, and other travel charges. For further information regarding travel expenses, please refer to the applicable collective bargaining agreement or "Rules Governing Paid Leave And Other Benefits For Managers And Confidential Employees" also known as the "Red Book." This document is accessible on the HRD section of the ANF portal, http://www.mass.gov/anf.

Please note some collective bargaining agreements have additional benefits. http://www.hrd.state.ma.us/agency_services/AS_Manage_Workforce/Rules_and_Guidelines/collectivebargaining.htm

Please check with your Human Resources department on your eligibility for other expenses being paid or reimbursement for items such as clothing allowances, meals, or equipment.

Please see your supervisor or the ITD Employee Portal to obtain a reimbursement form. Reimbursements are deposited to your direct deposit account and your pay advice will

reflect the reimbursement. Therefore, it is important that you update your Payroll Manager if your bank account information changes.

4.4 Out of State Travel Authorization

MGL c.30 s.25B provides that no officer or employee of the Commonwealth may travel *out-of- state* at public expense except in accordance with rules and regulations established by the Secretary for Administration and Finance. Additional information on out-of-state travel can be found on the ANF web portal, www.mass.gov/anf, choose "Budget, Taxes & Procurement", then choose "Administrative Bulletins".

All out-of-state travel requires the submission of a completed Out of State Travel Authorization Form (TAF) for approval by the Agency Head and appropriate Cabinet Secretary. A copy of the TAF is posted to the ITD employee portal, www.mass.gov/itdemployee, click on "Finance and Procurement", and scroll to "Forms & Publications" section on right hand side of page.

4.5 Military Pay Provision

If you serve in the Armed Forces of the Commonwealth (Massachusetts National Guard) including participating in an Annual Tour of Military Duty, you will receive regular state pay without losing any ordinary compensation that you would have received, up to a maximum of 34 days per state fiscal year (July 1 to June 30). You must meet the conditions outlined in the Massachusetts General Law, Chapter 33, sections 38, 40, 41, 42, 59, and 60 to qualify for this benefit.

If you participate in an Annual Tour of Military Duty as a member of a reserve component of the Armed Forces of the United States, you will receive regular state pay without losing any ordinary compensation that you would have received, up to a maximum of 17 days per federal fiscal year (October 1 to September 30). You must meet the conditions outlined in the Massachusetts General Law, Chapter 33, section 59 to qualify for this benefit.

In accordance with Chapter 173 of the Acts of 2003, the Military Pay Act provides that if you are called for active military service after September 11, 2008 in the Army National Guard, the Air National Guard or a Reserve Component of the Armed Forces, you may be entitled to compensation equal to the difference between your state pay and your military pay if your state base pay is higher.

Please notify your Human Resources Director in advance if you will be participating in any military duty.

4.6 Prior Approval to Earn Compensatory Time

ITD bargaining unit employees under contracts which allow for accrual of compensatory time must receive prior written approval from their supervisor to earn compensatory time.

4.7 Overtime Pay for Non-Management Employees

4.7.1 Prior Approval to Work Overtime

ITD employees must request and obtain pre-approval prior to working any overtime. Approval is requested through a change order ticket in the ITD work management

system. Supervisors are responsible for moving overtime tickets to the appropriate budget approver based on the funding source for the overtime. Budget approval will come from the Service Account Manager for customer funded overtime and from the senior budget approver in the group for internal projects. The senior budget approver for the group, or "Officer", is the manager who reports directly to the Agency Head.. Officers may delegate budget approval to their reports as they see fit. Employees must notify their supervisor immediately after overtime is worked, and enter the hours in Clarity. The supervisor will then complete their task in Service Desk to move the Change Order to the appropriate Officer/designee, or Service Account Manager for agency-funded overtime. The Officer/designee or Service Account Manager will forward the ticket to the Payroll Manager so that the overtime can be paid.

Detailed guidelines for how to submit Overtime Approval Requests are posted to the ITD Employee portal – www.mass.gov/itdemployee, click on "Payroll & Benefits", then choose "Guide to Submitting OT Approvals".

4.7.2 Calculation of Overtime Pay

Rules governing calculation of overtime pay for non-management staff are governed by the language in the NAGE contract. A summary has been provided below. Any questions regarding this summary or language may be directed to the Human Resource Department at ITD.

Full time employees are compensated at the rate of time and one-half his/her regular hourly rate of pay for authorized overtime work performed in excess of forty (40) hours per week. An employee whose regular workweek is less than forty (40) hours shall be compensated at his/her regular rate for authorized overtime work performed up to forty (40) hours per week that is in excess of his/her regular workweek.

An employee whose regular workweek is less than thirty-seven and one-half (37.5) hours will be compensated at the rate of time and one half his/her regular hourly rate of pay for authorized overtime work performed in excess of eight (8) hours in his/her regular workday except that an employee whose regular workday is more than eight (8) hours shall be compensated at the rate of time and one half his/her regular hourly rate of pay for authorized overtime work performed in excess of his/her regular workday.

With the exception of paid sick leave, all time for which an employee is on full paid leave status shall be considered time worked for the purpose of calculating overtime compensation. However, an employee who uses sick leave during the same work week in which he/she works mandatory overtime shall have the opportunity to replace up to three (3) shifts per fiscal year of sick leave with his/her available personal leave, vacation leave, accrued compensatory time or holiday compensatory time. Furthermore, up to two (2) days of sick leave may be counted toward such overtime calculation if the employee submits medical evidence from a licensed Physician, Physician's Assistant, Nurse Practitioner, Chiropractor or Dentist that he/she has personally examined the employee and determined that the employee was unable to perform his or her duties due to the specific illness or injury on the days in question.

4.8 Payroll Deductions

For information on tracking your payroll deductions, please refer to the section on "Payinfo".

4.8.1 Mandatory Payroll Deductions

Name	Description
Federal Tax	Complete W-4 form
State Tax	Complete M-4 form
Medicare	1.45% of " Gross pay" if you were hired on or after April 1, 1986
Retirement – Pre Tax (or alternative OBRA for contract employees)	The first $2,000 is subject to federal tax, not subject to state tax; your contributions in excess of $2,000 are subject to both federal and state tax.
Additional Retirement – 2% - Pre Tax	An additional 2% retirement contribution will be deducted bi-weekly from your paycheck if you have regular annual compensation over $30,000 and you entered state service on or after January 1, 1979.
Agency Service Fees or Union Dues	This applies only if you are covered by a collective bargaining agreement.

4.8.2 Optional Payroll Deductions

Basic and Optional Life Insurance
Health Insurance
GIC Dental and Vision (Managers and Confidential employees)
Long-Term Disability Insurance
Deferred Compensation (extra money towards retirement)
Dependent Care Assistance Program (DCAP) – Pre-Tax
Health Care Spending Account (HCSA) - Pre-Tax HCSA/DCAP Administrative Fee – Pre-Tax
Commonwealth of Massachusetts Charitable Campaign (COMECC)
Savings Bonds
Personal deduction to a credit union, bank, U.Fund (college savings plan)
MBTA Pass Program
Union sponsored plans including dental and vision (contact union for more information)

4.9 Salary Increases

If you are an employee covered by a collective bargaining agreement, overall salary rates are established through collective bargaining.

Generally, you advance to the next higher salary in your job grade in the salary chart, referred to as the next step, after each fifty-two (52) weeks of creditable service and if your performance is satisfactory. For most employees, this salary increase is received on their anniversary date, which is the date of their hire or the date of their last or most recent promotion.

If you are a manager, salary increases are determined by ANF and awarded based upon job performance. Performance reviews for manager occur in September; increases are effective October 1.

If you are in a Technical Pay Law (TPL) position, guidelines for issuance of salary increases are negotiated by ITD and HRD and require ANF approval..

If you are in an Intern position, your pay is governed by the ranges approved by the rates under Massachusetts General Laws, Chapter 29, Section 29, determined by the Secretary for Administration and Finance as recommended by the Chief Human Resources Officer (CHRO.)

4.10 Stand-By/Call Back

An employee who is required by ITD to be available on a stand by basis to report to duty or respond to page or phone call when necessary will receive stand-by pay of $17.50 for each stand-by period. The stand-by period is fifteen hours in duration for any night stand-by duty, and nine hours in duration for any day stand-by duty. If any employee assigned to stand-by duty is not available to report to duty when contacted, no stand-by pay shall be paid to the employee for the period. If an employee is on standby for one week, s/he is entitled to $157.50 in standby pay ($17.50 per shift from Monday – Friday and 2 shifts for Saturday and Sunday).

Any employee who is on Stand-by duty coverage during a holiday which is not subject to skeleton operational coverage by other members of their operational unit is entitled to an additional payment of $17.50 for the coverage of that holiday. This additional Stand-by period payment will not be extended for holidays which are "floaters" or otherwise include on-site operational coverage of that unit's function during the holiday.

If the employee receives a call he or she may be entitled to Call Back Pay. Multiple calls within the two hour period are considered one call back event. (A call back event is defined as an employee receiving multiple calls within a 2 hour period or one problem that took up to 2 hours to resolve.) Calls outside of the two hour period are considered a separate call back event. If the problem takes more than two hours to resolve the employee will be paid at the appropriate overtime rate (for example, if the problem took three hours to resolve, it is considered one call-back event plus one hour).

For employees on a 37.5 hour work week, the first 2.5 hours of call-back pay will be straight hourly pay (or straight hour for hour comp time). Time worked over 40 hours per week will be compensated at a rate of one and one-half times the hourly rate (or one and one-half hours of comp time per hour worked). Sick leave is not considered time worked for OT purposes.

All Stand By and Call Back events must be indicated in Clarity and must be approved by the appropriate supervisor as well as the Chief Financial Officer.

The guiding principle for pay for call back events is whether a substantive task has been performed and whether the employee has been "inconvenienced" as anticipated in the collective bargaining agreement.

Examples of when Call Back situations may result in compensation:

Employee is asked a question or is informed of an incident that takes substantive research or investigation to answer, or employee needs to read documentation or login to the network or application to answer or resolve incident

Employee on standby calls someone else for information or assistance and that individual completes the substantive components of the task – second individual may be paid for time worked

Examples of when Call Back situations may not result in compensation:

Employee is asked a question or is informed of a problem they know they cannot answer – issue needs to be escalated to manager or a more experienced staff person (If some

activity was completed before deciding the problem needed to be turned over to someone else, there may be pay if there was a legitimate effort to complete the task.)

Second person is called by the employee paged by Operations for some information but does not deal with operations or complete any substantive effort to complete a task or resolve an incident

Section 5: Benefits

5.1 Adoption Tuition Incentives

The Tuition Remission provision of the Massachusetts Department of Social Services (DSS) Adoption Assistance Program provides free tuition at Massachusetts State and community colleges and at the University of Massachusetts to DSS children adopted by full-time or regular part-time state employees on or after January 1, 1995. There is a minimum length of service requirement for state employees and the level of tuition reimbursement may vary depending on course type. Please see Executive Order 417 for more details. Full text of all Executive Orders is accessible via the website for the Governor's Office, www.mass.gov/gov . You may also use the link below: http://www.lawlib.state.ma.us/source/mass/eo/eotext/EO417.txt

5.2 Deferred Compensation / 457b (Optional)

The Massachusetts Deferred Compensation SMART Plan is a supplemental retirement savings program offered by the State Treasurer and administered by a private financial services provider. SMART stands for Save Money and Retire Tomorrow. Authorized under Section 457 of the IRS, the SMART Plan allows you to save and invest before-tax dollars for retirement through voluntary salary deferrals. You decide, within IRS legal limits, how much of your income you want to defer as this account is solely funded by your own contribution and does not receive contributions from your employer. Your Payroll Department will reduce your paycheck by that amount before income taxes and your contributions will be invested, per your instructions, to one or more of the investment options offered under the Plan. There is no employer contribution match. A nominal monthly administrative fee will be charged to your account. Contributions and any earnings that accumulate over the years are not taxed until you receive them. Distributions are allowed upon separation of service, death or incurring of an unforeseeable emergency as defined by the IRS. Participating in the SMART Plan will not replace or reduce any pension or Social Security benefits. For more information please contact your human resources office or the SMART Plan.

5.3 Dental/Vision Insurance (Optional)

If you are a manager or confidential employee, please contact your Human Resources department for information on enrolling in the dental/vision plan offered by the Group Insurance Commission. The plan primarily covers managers, legislators, legislative staff and certain Executive Office staff.

If you are an employee covered by a collective bargaining contract, please contact your union representative for more information on enrolling in a dental and vision plan that is offered by a private vendor and funded by a jointly administered labor-management Health and Welfare fund

5.4 Dependent Care Assistance Plan (DCAP) (Optional)

The Dependent Care Assistance Plan, offered by the Group Insurance Commission, allows employees to pay for certain dependent care expenses, such as child care and day camp, with before-tax dollars. Participating in DCAP can significantly reduce your federal and state income taxes. There is a nominal monthly pre-tax administrative fee.

It is important to estimate your expenses carefully, as the Internal Revenue Service requires that any unused funds in a participant's account at plan year-end be forfeited. Active state employees including contract employees who work half-time or more and have employment-related expenses for a dependent child under the age of 13 and/or a disabled adult dependent are eligible for DCAP. The fall open enrollment period takes place in November and December for the following calendar year. You must re-enroll each year in the plan. For more information, go to the GIC website at www.mass.gov/gic, and search using the term "DCAP".

5.5 Employee Assistance

Live and Work Well Website

To assist you with dealing with stress, the GIC, in conjunction with our mental health and substance abuse provider, United Behavioral Health (UBH), offers you an online resource. Use this GIC members-only site to:

Discover interactive learning programs on a variety of work and wellness topics including stress management, team building, and balancing home and work.

Try dozens of useful calculators and planning tools

Search for resources

Explore an extensive library of health and wellness articles and publications

The web address is: https://www.liveandworkwell.com/public/

10910 is your Access Code.

Legal Referral Services

Free Legal Referral Services are available to the following health plan members:

Commonwealth Indemnity Plan (includes Community Choice, OME and PLUS) and Navigator by Tufts Health Plan.

The Law Phone Legal Services is offered by United Behavioral Health and this service provides:

Free telephone consultations with an attorney.

A free 30-minute "face-to-face" consultation with an attorney.

A 25 percent discount for additional services provided by an attorney.

LawPhone can help you when you need legal information or encounter any legal problem. It is also useful when legal advice is needed or help is needed for drafting legal documents. In addition, LawPhone can assist you for self-representation in court or if you have received notice of a suit, summons, or subpoena to appear in court.

To be connected with LawPhone, call UBH at 1-888-610-9039 (TDD: 1-800-842-9489).

The Group Insurance Commission web site also maintains a list of resources and articles for all employees to access. Go to www.mass.gov/gic and search on "manage your health".

5.6 Extended Illness Leave Bank (EILB) (Optional)

You may be eligible to join the EILB, which may be used only when you experience a serious illness or injury. This is a voluntary program that allows you to receive benefits for yourself or assist other employees experiencing prolonged illness or injury who otherwise would be forced to take an unpaid leave of absence. Membership in EILB is limited to specific open enrollment periods. Members must donate leave time annually to maintain enrollment. Please contact your Human Resources department http://www.hrd.state.ma.us/employee_services/ES_Emp_Bene/eilb.htm

if you would like to receive more information on membership and withdrawal criteria.

5.7 Health Care Spending Account (HCSA) (Optional)

The HCSA program (http://www.mass.gov/gic and search on "HCSA") , offered through the Group Insurance Commission, allows you to pay for certain non-covered health related expenses with pre-tax dollars, thus reducing your federal and state income taxes. Expenses must be medically related. Examples include physician office and prescription drug co-payments, medical deductibles and coinsurance, eyeglasses and contact lenses not covered by your health or vision plan, orthodontia and dental benefits not covered by your dental plan, and most over-the-counter drugs.

If you participate in the HCSA, you will be charged a nominal monthly pre-tax administrative fee. It is important to estimate your expenses carefully, as the Internal Revenue Service requires that any unused funds in a participant's account at plan year-end be forfeited. You must be eligible for GIC benefits to be eligible for the HCSA plan and the waiting period is the same as for health benefits (see Health Insurance). The fall open enrollment period takes place in November and December for the following calendar year. You must re-enroll each year in the plan. Please contact your Human Resources Department for more information about this program.

5.8 Health Insurance (Optional)

The Group Insurance Commission (GIC) administers health insurance coverage. You can either elect to participate in an insurance plan that is a Health Maintenance Organization (HMO), a Preferred Provider Organization (PPO), Point of Service Plan (POS), or an Indemnity Plan. Please see the GIC's Benefit Decision Guide (http://www.mass.gov/gic and scroll to the "Forms and Publications" section) for detailed information regarding health insurance options.

If you enroll in this optional benefit, your health insurance becomes effective on the first day of the month after you have been employed for two (2) full calendar months. For example, if an employee starts on January 5, his/her health insurance would be effective April 1 – two calendar months – February and March – after start date. Premiums are deducted on a bi-weekly basis from your pay advice. The percentage of the premium contributed by the employee depends on the date of hire or annual salary and currently ranges from 15% to 25%.

If you do not elect to carry health insurance within 10 days of employment, you will generally not be eligible to obtain insurance until the annual enrollment period which usually occurs during the months of April and May with coverage taking effect on July 1st. Certain circumstances (i.e. loss of coverage elsewhere) may warrant a waiver of this

restriction. Any change selected during the annual enrollment period is effective July 1st of that year

5.9 Holidays

The State observes the following paid holidays:

January 1: New Year's Day
3rd Monday in January: Martin Luther King Day
3rd Monday in February: President's Day
*March 17: Evacuation Day (Suffolk County)
3rd Monday in April: Patriots Day
Last Monday in May: Memorial Day
*June 17: Bunker Hill Day (Suffolk County)
July 4: Independence Day
1st Monday in September: Labor Day
2nd Monday in October: Columbus Day
November 11: Veterans Day
4th Thursday in November: Thanksgiving
December 25: Christmas Day

*Offices outside of Suffolk County must remain open on Suffolk County holidays. If you work a Suffolk County holiday, you are entitled to a day off with pay, to be used within a certain amount of time following the holiday as approved by your supervisor. Please see your collective bargaining agreement or the Red Book for details.

If a holiday falls on a Sunday, the following Monday is observed as the holiday. If a holiday falls on a Saturday, most employees will be given the preceding Friday off. State law requires, however, that state offices remain open on a Friday that precedes a Saturday holiday. This means that a sufficient number of employees will be required to work to provide coverage, and those who do so will be given an additional day off, within a certain amount of time, with the approval of their supervisor. Whenever possible, the following Monday should be used as the additional day off.

5.10 Lactation Accommodation/Mother's Room

The Bureau of State Office Buildings provides a private space for nursing mothers to use during working hours. This room is located on the 12th Floor of 1 Ashburton Place. Please contact the BSB for more information on access to this room. For information on accommodations for nursing mothers in the MITC facility, please contact a member of ITDs Human Resource Unit.

5.11 Leaves

5.11.1 Absence From Work Without Pay

Absence from work without pay (authorized or unauthorized) may affect leave accruals, vacation status, salary adjustments, GIC benefits, and/or other benefits. An employee on

unpaid leave may need to pay insurance premiums directly to the Group Insurance Commission. Absence from work with pay may also affect GIC benefits.

5.11.2 Bereavement Leave

You may take up to four (4) days paid leave for the death of certain family members and other individuals. Please consult your collective bargaining agreement or contact your Human Resources Director for further information if you need to use this type of leave time.

5.11.3 Blood Donation Leave

Any manager, confidential, or bargaining unit employee may take up to four (4) hours leave of absence with pay, subject to approval by their supervisor(s), for the purpose of donating blood to the Massachusetts State Employees Blood Program. The leave must be taken on the day that the blood donation occurs and employees may be permitted to donate up to a maximum of five (5) times each year during the period of October 1 through September 30. Employees who donate blood five times a year are also allowed up to four (4) hours leave of absence with pay to attend the annual Massachusetts State Employees Blood Program award ceremony.

5.11.4 Bone Marrow Donation /Organ Donor Leave

For participation in a bone marrow donor program or an organ donor transplant, a maximum of thirty (30) days of leave of absence with pay shall be granted to undergo the medical procedure and for associated physical recovery time.

5.11.5 Court/Jury Duty Leave

You are entitled to leave with pay when called for jury service or when summoned as a witness on behalf of any city, town, county of the Commonwealth, or the state or federal government.

If you receive jury fees for jury service and present the appropriate court certificate of service, you shall either:

Retain such jury fees in lieu of pay for the period of jury service, if the jury fees exceed your regular rate of compensation for the period involved; or

Remit to your agency the jury fees if less than your regular rate of compensation for the period involved.

5.11.6 Disaster Volunteer Leave

With agency head and supervisor approval, all Executive Branch employees who are American Red Cross Disaster Relief Volunteers may serve as a paid disaster volunteer up to 15 calendar days in a calendar year.

5.11.7 Domestic Violence Leave

You may be entitled to domestic violence leave if you and/or your children are victims of domestic violence and need to go to court, attend medical appointments, etc. This leave can be paid and/or unpaid, depending upon the length of the leave. If you have any questions, please consult your Human Resources Representative for the name of your agency's Domestic Violence Coordinator who will handle your situation confidentially.

5.11.8 Family and Medical Leave Act

You may be eligible to receive up to twenty-six (26) weeks per year, of unpaid, job protected leave for certain family and medical reasons under the Family and Medical Leave Act of 1993 (FMLA). However, the Commonwealth provides you with a more extensive Family and Medical Leave benefit. Certain kinds of your paid leave may be substituted for unpaid leave in accordance with various collective bargaining agreements or RedBook. Please see your applicable union contract or the Red Book for further details. Additional information is available on the HRD website, www.mass.gov/hrd. Type "FMLA" in the search window for more information.

5.11.9 Parental/Family Leave

As specified in the "Rules Governing Paid Leave and Other Benefits for Managers and Confidential Employees" (or Redbook), and the NAGE Collective Bargaining Agreement, an employee shall receive his/her regular salary for 10 days of leave , at a time requested by the employee, during family leave taken in conjunction with the birth, adoption or foster placement of a child. These 10 days of paid leave may be used on an intermittent basis over the 12 months following the birth, adoption or placement, except that the leave may not be charged in increments of less than one day.

5.11.10 Personal Leave

If you are a full-time or regular part-time manager or confidential employee, you will be awarded three personal days on January 1 of each year. These days will be prorated for the year if you are a part-time employee or if you were hired on or after April 1.

Most full-time or regular part-time employee covered by a collective bargaining agreement will be awarded three personal days on January 1 of each year. These days will be prorated for the year if you are a part-time employee or if you were hired on or after April 1.

If you have unused personal leave at the end of the calendar year or if you separate from state service, this unused time is forfeited and you will not receive compensation for this time. You can select to donate any unused personal time that would be forfeited to the Extended Illness Leave Bank (EILB.)

5.11.11 Sick Leave

You accrue sick leave credits on a monthly basis. If you are a part-time employee, your accrual rate will be prorated accordingly. If you experience time off the payroll without pay, your sick leave accrual rate may be affected. Please consult your respective collective bargaining agreement or Red Book for specific circumstances, conditions and/ or limitations of this benefit. These documents are available on the Human Resources Division web site at http://www.mass.gov/hrd/ or www.hrd.state.ma.us.

Upon an employee's retirement (or upon their death) employee (or estate) will receive 20% of the value of their current sick leave balance

5.11.12 Small Necessities Leave

In accordance with the provisions of Massachusetts General Laws, Chapter 149, Section 52D, employees shall be entitled to a total of 24 hours of unpaid leave during any 12

month period, in addition to leave available under the Family and Medical Leave Act of 1993, for the following purposes:

to participate in school activities directly related to the educational advancement of your son or daughter, OR

to accompany your child or elderly relative to routine medical or dental appointments, or for other professional health care services

If you have accumulated sick, personal, or vacation credits at the commencement of your Small Necessities Leave, you may use such credits for which you may be eligible under the applicable rules. The Act does not require the Commonwealth to provide paid sick leave or paid medical leave in any situation where the Commonwealth would not normally provide such paid leave.

5.11.13 Vacation Leave

You accrue and receive credit for vacation at the end of each full calendar month you have worked. The length of your creditable state service determines the number of vacation hours you are credited. During a transitional year, a year when you change to a higher accrual rate, you will receive your new vacation status on the July 1st that precedes your creditable service date.

Years of Creditable Service	37.5 hrs/wk	40.0 hrs/wk
Less than 4 ½ years*	6.25	6.667
4 ½ yrs but less than 9 ½ yrs	9.375	10.0
9 ½ yrs but less than 19 ½ yrs	12.5	13.333
19 ½ yrs or more	15.625	16.667

*If you are a manager or confidential employee, you will earn 7.5 or 8.0 hours per month if employed less than 4.5 years. Subject to the approval of the Chief Human Resources Officer, if you are a newly hired manager or confidential employee who has completed one month of state service, you have the option to request an advance of no more than five vacation days and/or you may start with a higher vacation accrual rate based on comparable prior work experience. If you opt to receive an advance of vacation credits, you shall not accrue additional vacation credits until sufficient time has accrued to offset the amount of vacation credits that were advanced. Please consult the Red Book for specific rules governing this advance. If you are a part-time employee, you will earn your vacation leave on a pro-rated basis.

Time off the payroll without pay may affect your vacation status and accrual rate. Please refer to your collective bargaining agreement or Red Book for more information. You may carry over hours of unused vacation time (with certain limitations) and any vacation time that can't be used and would be forfeited can also be donated to ELIB.

Upon leaving state service an employee will be compensated for the value of their unused accrued vacation time.

5.11.14 Volunteer Leave Program: SERV

SERV (State Employees Responding as Volunteers) is an employee benefit available to eligible employees in the Executive Branch who have at least six months of state service. With supervisor approval, an employee may volunteer during regular work schedule up to one day per month at an approved Massachusetts non-profit organization (7.5 or 8 hours/month; pro-rated for part-time employees). Eligible areas include:Education, Youth Mentoring, Public & Charter Schools, Health & Human Services, Public Safety and Environment.

More information about the SERV program is available on HRDs website, www.mass.gov/hrd, clicking on "Employee Programs and Training" and then clicking on "SERV".

5.11.15 Voting Leave

Full-time and regular part-time employees whose hours of work preclude them from voting in a town, city, state, or national election shall, upon prior written approval of the Appointing Authority, be granted a voting leave with pay not to exceed two hours, for the sole purpose of voting in such election.

5.11.16 Workers' Compensation Leave

Workers' Compensation Insurance is coverage, mandated by state law, Massachusetts General Laws, Chapter 152 that provides you salary protection due to work-related injuries and illnesses. The Human Resources Division (HRD) Workers' Compensation Section is currently the designated administrator for Commonwealth employees except for uniformed State Police. If you suffer on-the-job injuries or job-related illness, and your claim is approved, you may receive benefits to cover medical costs and offset loss of wages during your period of disability.

If you are involved in or witness an accident at work, you should report it immediately to your supervisor. Prepare an Accident Report ("First Report of Injury - Form 101") as soon as possible. Failure to report on-the-job injuries could jeopardize your right to workers' compensation. You will not receive compensation for injuries resulting from your serious or willful misconduct. If you submit a fraudulent claim, you will be subject to disciplinary action up to and including termination of employment.¶

5.12 Life Insurance (Basic and Optional)

Life insurance is offered through the Group Insurance Commission (GIC.) See your GIC Benefit Decision Guide (http://www.mass.gov/gic and scroll down to "Forms and Publications" on right of page to "Benefit Decision Guides") for additional information.

Basic Life Insurance: The Commonwealth offers $5,000 of basic life insurance as part of your health insurance plan. You may choose to enroll in basic life insurance without enrolling in the health insurance plan. You and the Commonwealth share the cost of this insurance.

Optional Life Insurance: This term insurance covers you and pays your designated beneficiaries in the event of your death or certain other catastrophic events. Employees pay 100% of the premium. As a new employee, you may enroll in Optional Life Insurance for a coverage amount of up to eight times your salary without the need for any medical review. If you do not elect optional life insurance coverage when first eligible, or do not elect the maximum amount available, you can apply at any time by completing a medical application for the insurance carrier's review and approval.

5.13 Long-Term Disability Insurance (LTD) (Optional)

LTD, offered by the Group Insurance Commission, is an income replacement program that protects you in the event you become disabled or are unable to perform the material and substantial duties of your job. It allows you to receive a portion of your salary on a tax-free basis.

If you are a new full-time or half-time employee, who works at least 18.75 hours in a 37.5 hour workweek or 20 hours in a 40 hour workweek, you may apply to enroll in the LTD plan without providing evidence of good health within 31 days of hire. If you do not enroll within 31 days of hire, you are eligible to enroll in the LTD plan at anytime but you will be required to provide evidence of good health for the vendor's approval to enter the plan. Employees pay 100% of the premium. For more information, go to www.mass.gov/gic and search on "long term disability".

5.14 Qualified Transportation Benefits Program (formerly the MBTA Pass Program)

Employees interested in information on obtaining pre-tax benefits for purchase of transportation services can contact Benefits Strategies via email at "info@benstrat.com" or visit their website at www.benstrat.com.

5.15 Retirement System

If you are a regular state employee (half-time or more), you are required to enroll as a member of the State Employees Retirement System administered by The State Board of Retirement. Contract employees and those who do not meet the membership criteria of this program are required to enroll in the Alternate Retirement Plan (OBRA). Under Massachusetts Law, the first $2,000 of combined Retirement and Medicare withholdings is pre-tax for state tax withholding purposes. Your date of hire and rate of pay determine the percentage rate of your bi-weekly retirement deduction.

Hired before January 1, 1975	5%
Hired on or between January 1, 1975 – December 31, 1983	7%
Hired on or between January 1, 1984 – June 30, 1996	8%
Hired on or after July 1, 1996 – present	9%
State Police hired on or after July 1, 1996 – present	12%

If you were hired on or after January 1, 1979, an additional 2% is deducted for retirement on the amount of your salary that exceeds $30,000.

Your deduction for the retirement system begins with your first pay advice. The Commonwealth does not contribute a specific percentage per employee towards this program; however the Commonwealth contributes an overall amount annually to the fund needed to cover any unfunded liability.

If you are a member employed on a full-time basis, you will earn one year of creditable service for each year of service completed. If you are a member employed on a less than full-time basis, you will earn an amount of service that equals your percentage of full-time service (i.e. creditable service is prorated.)

If you re-enter the System with funds on deposit or transfer from another Contributory Retirement System, you maintain your contribution level.

Generally, you will be eligible for retirement once you have 20 years of service or if you are at least age 55 with at least 10 years of service. If you meet all the eligibility requirements for retirement, you can retire with a retirement allowance up to 80% of the average of your highest 36 months of regular compensation. Earnings such as certain differentials may have been identified as "regular compensation" for retirement purposes. Social Security benefits may be affected by your state pension under federal law.

Because of the many variables connected with retirement, it is vital that you discuss your situation in advance with a Retirement Counselor at the State Board of Retirement. The contact information for the State Board of Retirement may be found in Appendix I.

5.16 Same Sex Marriage Benefits

Same sex spouses of Executive Branch employees are entitled to benefits such as GIC benefits (health insurance, etc), Family and Medical Leave (FMLA), Non-FMLA Leave, Tuition Remission for spouses, Sick Leave, Bereavement Leave, Domestic Violence Leave, Small Necessities Leave, "Sunshine Policy" on disclosure of immediate family members who are state employees. Contact Group Insurance Commission for questions on GIC benefits. Contact the Human Resources Division on all other questions on this policy.

5.17 Savings Bonds (Optional)

You may elect to enroll to purchase United States Savings Bonds at half their face value via a bi-weekly payroll deduction. Please note that if you enroll, there is a minimum level of bond that must be purchased. Once a sufficient amount of money has been deducted from your pay, your bond(s) will be mailed to your specified address.

5.18 Tuition Remission

You and your spouse may be eligible to participate in a tuition remission program. If approved, you may receive partial to full tuition remission (except for fees, books, and materials) for programs and courses taken on your own time at public community colleges, state colleges, and state university campuses (excluding the medical school at University of Massachusetts).

For additional information, go to HRDs website at www.mass.gov/hrd, scroll down to click on the "Employee Programs and Training" section in the center of the page, and choose "Tuition Remission".

5.19 U.FundSM College Investing Plan

To help families plan for the costs of higher education, the Massachusetts Educational Financing Authority (MEFA) established the U.FundSM College Investing Plan in 1999. Offered in partnership with Fidelity Investments, the U.Fund is flexible and affordable, and combines significant tax advantages with professional investment management. The U.Fund is designed for parents, grandparents or anyone interested in helping to provide for the higher education of a loved one. Whether the loved one attends a four-year public or private college, a two-year community college or vocational-technical school, or even graduate school anywhere in the United States, the U.Fund can help you prepare for the significant financial challenge that lies ahead. Then, when your child is ready for

college, you can use the funds to cover a wide range of qualified education expenses. For more information, please see this link: http://www.mefa.org

Appendices: ITD Workplace Policies

A. ITD HR Policy 2008-01 Effective 10/1/2008: Policy of Zero Tolerance for Sexual Assault, Domestic Violence and Stalking
B. ITD HR Policy 2008-03 Effective 8/1/2008: Policy of Zero Tolerance for Workplace Violence
C. ITD HR Policy 2009-01 Effective 9/1/2009: Policy Statement Prohibiting Workplace Discrimination:
D. ITD HR Policy 2006-01 Effective 7/1/2006: Sexual Harassment Policy
E. ITD HR Policy 2008-02 Effective 10/1/2008: Criminal Offender Record Information (CORI) Policy
F. ITD HR Policy 2006-02 Updated 9/1/2010: Telecommuting Policy
G. ITD HR Policy 2008-04 Updated 7/1/2010: Desktop Unit Management Policy
H. ANF Policy on the Use of Information Technology Resources Issued by ANF June 16, 1998
I. Enterprise Information Technology Policies

A. ITD HR Policy 2008-01 Effective 10/1/2008: Policy of Zero Tolerance for Sexual Assault, Domestic Violence and Stalking

Policy

The Commonwealth has a zero-tolerance policy for sexual assault, domestic violence, and stalking occurring within or outside the workplace. Effective immediately, it is the policy of the Information Technology Division (ITD) that all employees work in an environment free from all forms of sexual assault and domestic violence. Sexual assault and domestic violence undermine the integrity of the work place and the personal safety of the individual.

Authority

Executive Order 491 establishes a zero tolerance policy for sexual assault, domestic violence and stalking and requires state agencies to issue written policies and to provide copies of the policy to all employees. The Executive Order applies to all individuals employed on a full-time or part-time basis by the Office of the Governor or any state agency under the Executive Department.

Definition of Domestic Violence

Chapter 209A of the Massachusetts General Laws defines domestic violence as a form of abuse among family or household members, which includes those individuals who are or have been involved in a substantive dating relationship. Abuse is defined as the occurrence of one or more of the following acts between family or household members:

- attempting to cause or causing physical harm; or
- placing another in fear of imminent serious physical harm; or
- causing another to engage involuntarily in sexual relations by force, threat of force, or duress.

Family or household members are persons who:

- are or were married to one another;
- are or were residing together in the same household;
- are or were related by blood or marriage;
- have a child in common regardless of whether they have ever married or lived together; or
- are or have been in a substantive dating or engagement relationship.

Chapter 209A provides a victim protection from an abuser through the issuance of a restraining order. Such an order may order the abuser to refrain from abuse, to vacate the home, to comply with temporary custody and support orders, and/or to have no contact with the victim at all times. Although Chapter 209A orders are civil in nature, violations of certain provisions are criminal in nature and arrest following such violations is mandatory.

ITD will not initiate disciplinary action against an employee accused of abuse alleged to have occurred outside the workplace unless presented with an authentic copy of a document showing a judicial finding of probable cause that the employee committed an act of abuse against a family or household member. ITD may require an employee who

is an abuser to accept reassignment to a different geographic location, if ITD determines that such reassignment will help better ensure the safety of the victim or others in the workplace. While maintaining confidentiality to the extent practicable, ITD may consult with appropriate legal staff, human resource/labor relations directors and/or domestic violence professionals for guidance in these matters.

Definition of Sexual Assault and Stalking

"Sexual assault" includes any action causing another to engage in sexual relations by force, threat, or duress in violation of Chapter 209A or chapter 265 of the General Laws, or any other applicable law of the Commonwealth.

"Stalking" includes any pattern or series of acts, conduct or threats causing or intended to cause alarm or fear in violation of chapter 209A or chapter 265 of the General Laws, or any other applicable law of the Commonwealth.

ITD will not initiate disciplinary action against an employee accused of stalking or sexual assault alleged to have occurred outside the workplace unless presented with an authentic copy of a document showing a judicial finding of probable cause that the employee committed an act of stalking or sexual assault. ITD may require an employee who is a stalker or abuser to accept reassignment to a different geographic location, if ITD determines that such reassignment will help better ensure the safety of the victim or others in the workplace. While maintaining confidentiality to the extent practicable, ITD may consult with appropriate legal staff, human resource/labor relations directors and/or domestic violence professionals for guidance in these matters.

The Commonwealth's view of sexual assault, domestic violence, and stalking reflects, but is not limited to, the following considerations:

- A man as well as a woman may be the victim of sexual assault, domestic violence, or stalking, and a woman as well as a man may be the abuser.
- The victim does not have to be the opposite sex from the abuser or stalker.

The Director of Human Resources shall:

- When appropriate, ensure written workplace safety plans are completed in response to confirmed reports of domestic violence, sexual assault, and stalking;
- When appropriate, while maintaining confidentiality to the extent practicable, work with victims in consultation with ITD's domestic violence coordinator, HR personnel, and/or Legal Counsel in addressing workplace safety and security plans that may impact victims and/or co-workers.
- Respect the privacy of victims and perpetrators and preserve confidentiality at all times, to the extent possible, in dealing with situations involving sexual assault, domestic violence or stalking;
- When notified of a restraining order in effect, utilize all reasonable efforts to address the employee's concerns about safety and report any workplace violations of such order to the police.

ITD Employees shall:

- Refrain from participating in any form of domestic violence, sexual assault, or stalking either within or outside the workplace;
- Cooperate in the investigation of alleged domestic violence, sexual assault, and stalking by providing information they possess concerning such matters;
- Report behavior in the workplace which they believe to be sexual assault, domestic violence, or stalking to their supervisor, or the police when appropriate.

Protection to domestic violence, sexual assault, and stalking victims

ITD recognizes that victims of domestic violence, sexual assault, and stalking may suffer from physical, mental, emotional, and sexual abuse. In an effort to afford victims of domestic violence, sexual assault, and stalking the ability to protect themselves and their families, and to ensure the safety of all employees, ITD has established the following policies:

- An employee who is a victim of domestic violence, sexual assault or stalking, or whose children are victims (where the employee is not the abuser) shall be entitled to up to fifteen (15) days of paid leave per calendar year for the purposes of counseling, obtaining medical treatment, attending legal proceedings, or carrying out other necessary activities resulting from domestic violence, sexual assault, or stalking.
  - The fifteen (15) days of paid leave will not be charged to sick, vacation or personal leave accrual.
- An employee who is a victim of sexual assault, domestic violence, or stalking and/or whose children are victims and the employee is not the abuser may be granted up to six (6) months of unpaid leave, where the employee requests such leave as a result of domestic violence, sexual assault or stalking. Leave accruals and insurance benefits shall be handled in the same way as is done for any other type of leave without pay. Upon the employee's return from leave, ITD shall restore the employee to the same position or to an equivalent position, with equivalent employment benefits, pay, and other terms and conditions of employment, provided that the employee has not been displaced from his/her position in the interim due to a reduction in force.
- Due to the emergency nature of leave requests, the employee may not be able to provide such documentation. However, when appropriate, agencies may request the following documentation:
  - A judicial finding of domestic violence, such as a 209A restraining order or pending criminal charges;
  - A signed letter from a district attorney's office, police department, or district, probate, or superior court;
  - Signed affidavits from third parties having knowledge of the abuse.
- To the extent possible, all documentation submitted shall be kept in a secure and confidential manner so as to respect the employee's right to privacy.
- A victim of domestic violence, sexual assault, or stalking is strongly encouraged to notify ITD of the existence of a restraining order protecting the employee. Upon such notification, ITD shall make all reasonable efforts to enforce the restraining order in the workplace. Such efforts may include:

    - Notifying security personnel of the identity of the person against whom the order is issued (defendant);
    - Providing security personnel with a photograph or other identifying information, such as motor vehicle information;
    - After notifying the employee, having the employee's calls screened;
    - Moving the employee's workstation away from an unsecured entrance.
- If ITD becomes aware that an active restraining order protects an employee, the agency may offer that employee a reassignment to a different geographical location. Where the victim has requested reassignment, ITD shall give the request top priority.
- ITD shall immediately notify the police if a violation of a restraining order occurs at the workplace.
- ITD will provide a list of domestic violence and sexual assault assistance programs, including the state-wide Safe-Link Hotline emergency hotline number, to employees who are victims of domestic violence, sexual assault, or stalking to assist them in finding available services.

Procedures for Investigating and Disciplining Abusers

ITD takes all instances of sexual assault, domestic violence, and stalking seriously. The following are guidelines for disciplining abusers:

- ITD shall immediately report any incident of domestic violence, sexual assault or stalking that occurs in the workplace, including violation of 209A restraining orders, to the appropriate law enforcement authorities.
- ITD must follow existing provisions in the collective bargaining agreements when disciplining abusers.
- ITD will consult with appropriate legal staff, human resource/labor relations directors and or domestic violence professionals for guidance in these matters.
- All investigations of domestic violence, sexual assault, or stalking policy violations alleged to have occurred within the workplace will be conducted in a manner to protect the confidentiality of the alleged victim, the alleged abuser and all witnesses. All parties involved in the proceedings will be advised to maintain strict confidentiality.
- Acts of domestic violence, sexual assault, or stalking, regardless of where they occur, will not be tolerated and may result in discipline, including, but not limited to:
    - An oral warning or reprimand;
    - A written warning or reprimand to be placed in a personnel file;
    - Required completion of a certified batterer intervention program;
    - Suspension or termination; or
    - Any combination of the above.
- Incidents of domestic violence, sexual assault, or stalking resulting in the conviction of a felony within the past five years, may be used as a factor in hiring determinations.
- As with all other such actions, disciplinary actions taken against abusers become part of their work history and will be considered when selecting employees for promotion, new work assignments and other types of personnel actions.

B. ITD HR Policy 2008-03 Effective 8/1/2008: Policy of Zero Tolerance for Workplace Violence

Policy

Workplace violence undermines the integrity of the workplace and the personal safety of the individual employee. Therefore, the Commonwealth maintains a zero tolerance policy for workplace violence. Effective immediately, it is the policy of the Information Technology Division that all of its employees work in an environment free from workplace violence.

Authority

Executive Order #442 establishes a zero tolerance policy for workplace violence and requires state agencies to promptly disseminate written copies of the policy to all employees. The Executive Order applies to individuals employed on a full time or part time basis by the Office of the Governor or any state agency under the Executive department.

Definition of Workplace Violence

For the purposes of this policy, "workplace" is defined as:

Any Commonwealth owned or leased property;

Any location where Commonwealth business is conducted;

Commonwealth vehicles or private vehicles being used for Commonwealth business;

In addition, workplace violence can occur at any location if the violence has resulted from an act or decision made during the course of conducting Commonwealth business.

Workplace violence includes but it not limited to the following:

Physical assault and/or battery;

Threats and/or acts of intimidation communicated by any means that cause an employee to be in fear of their own physical safety or that of a colleague;

Disruptive or aggressive behavior that places a reasonable person in fear of physical harm and/or that causes a disruption of workplace productivity; and/or

Property damage.

Violent behavior can include actions or communication in person, by letter or note, telephone, fax, or electronic mail. Incidents of workplace violence may be acted out individually or take place between employees, employees and clients/customers, employees and acquaintances/partners and employees and the general public.

ITD CIO and Director of Human Resources shall:

When necessary, notify state/and or local police in response to serious incidents of workplace violence;

Establish a Safety Incidence Team comprised of senior executive staff representing agency human resources, labor relations, security, training, and legal to devise and review policies, procedures and safety protocols, and to ensure consistent, coordinated responses to acts of workplace violence;

Ensure written workplace protection plans are devised for employees who are victims of workplace violence; and implement any necessary workplace safety protocols designed to further protect employees from harm

ITD Supervisors and Managers shall:

Report all incidents to the Director of Human Resources to insure appropriate documentation and swift investigation of reports of workplace violence

ITD Employees shall:

Ensure that they do not participate in any form of workplace violence

Cooperate in the investigation of alleged workplace violence; and

Report behavior in the workplace they believe to be workplace violence to their supervisor, or the police when appropriate.

Procedures for Investigation and Disciplining Perpetrator

As stated above, the Commonwealth maintains a zero tolerance policy for workplace violence. The Information Technology Division takes all instances of workplace violence seriously. The following are guidelines for disciplining perpetrators:

ITD shall immediately report incidents of workplace violence that include physical assault and/or battery, and/or threats to do physical harm, to the appropriate law enforcement authorities;

All investigations of workplace violence will be conducted in a manner that is sensitive to the safety concerns and privacy of the victim(s), the perpetrator, and all witnesses.

ITD must follow existing provisions in the collective bargaining agreements when disciplining perpetrators;

Acts of workplace violence are among the most serious forms of misconduct and may result in discipline commensurate with the severity of the misconduct, including, but not limited to:

- An oral reprimand
- A written reprimand to be placed in the perpetrator's personnel file
- Suspension, demotion, or termination, or
- Any combination of the above**.**

In the interim, between a charge and the final disposition of a workplace violence case, the CIO may take action to address employees' safety concerns. Depending on the severity of the charge, such action may include placing the alleged perpetrator on leave with or without pay.

In addition to the measures mentioned above, disciplinary measures may include the successful completion of counseling, anger management education or other equivalent programs.

C. ITD HR Policy 2009-01 Effective 9/1/2009: Policy Statement Prohibiting Workplace Discrimination:

The following policy statement is included in this document as submitted with the Information Technology Division Affirmative Action Plan for Fiscal Years 2010 and 2011:

The Information Technology Division prohibits discrimination in employment on the basis of race, color, religious creed, national origin, ancestry, sex, sexual orientation, Vietnam Era Veteran status, age and disability.

I, Anne Margulies, Assistant Secretary and Chief Information Officer of the Information Technology Division, recognize that when the effects of employment practices, regardless of their intent, discriminate and create adverse impact against any group of people action must be taken to ensure that the Agency values employee Diversity, and affords equal opportunity through affirmative action.

Under the legal authority of: Massachusetts General Laws Chapter 151B; Executive Order 478; the Equal Pay Act of 1963; Title VI and Title VII of the Civil Rights Act of 1964; the Age Discrimination in Employment Act of 1967; the Equal Employment Opportunity Act of 1972; the Civil Rights Act of 1992; Section 504 of the Rehabilitation Act of 1973; the Americans With Disabilities Act of 1990; the Family and Medical Leave Act of 1993, I commit myself and my employees, within the context of these laws, to ensure equitable participation of minorities, women, Vietnam Era Veterans and persons with disabilities in all of its daily operations.

This policy applies to all employment practices and employment programs sponsored by this agency. The Agency shall review, investigate, and where necessary, initiate changes in its processes relative to facilities and programs accessible to the public, including the provision of reasonable accommodation for persons with disabilities. This policy shall also apply to the areas of recruitment, selection, promotions, termination, transfers, layoffs, compensation, training, benefits, reasonable accommodation, and other terms and conditions of employment.

I have designated my direct report, Ellen Wright, Director of Human Resources, as Diversity Director/Officer to implement all elements of this Equal

Opportunity/Affirmative Action (EO/AA) program. All management employees have personnel responsibility, and shall be designated specific tasks, relative to ensuring its successful implementation. All personnel shall be evaluated on the success of this program the same way as their performance is evaluated relative to other agency goals.

D. ITD HR Policy 2006-01 Effective 7/1/2006: Sexual Harassment Policy

I. Introduction

It is the goal of the Information Technology Division to promote a workplace that is free of sexual harassment. Sexual harassment of employees occurring in the workplace or in other settings related to their employment is unlawful and will not be tolerated by ITD. Further, any retaliation against an individual who has complained about sexual harassment or retaliation against individuals for cooperating with an investigation of a sexual harassment complaint is similarly unlawful and will not be tolerated. To achieve our goal of providing a workplace free from sexual harassment, the conduct that is described in this policy will not be tolerated and we have provided a procedure by which inappropriate conduct will be dealt with, if encountered by employees.

Because ITD takes allegations of sexual harassment seriously, we will respond promptly to complaints of sexual harassment and where it is determined that such inappropriate conduct has occurred, we will act promptly to eliminate the conduct and impose such corrective action as is necessary, including disciplinary action where appropriate.

Please note that while this policy sets forth our goals of promoting a workplace that is free of sexual harassment, the policy is not designed or intended to limit our authority to discipline or take remedial action for workplace conduct which we deem unacceptable, regardless of whether that conduct satisfies the definition of sexual harassment.

II. Definition Of Sexual Harassment

In Massachusetts, "sexual harassment" means sexual advances, requests for sexual favors, and verbal or physical conduct of a sexual nature when:

(a) submission to or rejection of such advances, requests or conduct is made either explicitly or implicitly a term or condition of employment or as a basis for employment decisions; or,

(b) such advances, requests or conduct have the purpose or effect of unreasonably interfering with an individual's work performance by creating an intimidating, hostile, humiliating or sexually offensive work environment.

Under these definitions, direct or implied requests by a supervisor for sexual favors in exchange for actual or promised job benefits such as favorable reviews, salary increases, promotions, increased benefits, or continued employment constitutes sexual harassment.

The legal definition of sexual harassment is broad and in addition to the above examples, includes other sexually oriented conduct, whether it is intended or not, that is unwelcome and has the effect of creating a work place environment that is hostile, offensive, intimidating, or humiliating to male or female workers.

While it is not possible to list all those additional circumstances that may constitute sexual harassment, the following are some examples of conduct, which if unwelcome, may constitute sexual harassment depending upon the totality of the circumstances including the severity of the conduct and its pervasiveness:

Unwelcome sexual advances -- whether they involve physical touching or not;

Sexual epithets, jokes, written or oral references to sexual conduct, gossip regarding one's sex life; comment on an individual's body, comment about an individual's sexual activity, deficiencies, or prowess;

Displaying sexually suggestive objects, pictures, cartoons;

Unwelcome leering, whistling, brushing against the body, sexual gestures, suggestive or insulting comments;

Inquiries into one's sexual experiences; and,

Discussion of one's sexual activities.

The complainant does not have to be the person at whom the unwelcome sexual conduct is directed. The complainant, regardless of gender, may be a witness to and personally offended by such conduct. The harasser may be anyone including a supervisor, a co-worker, or a non-employee, such as a recipient of public services or a vendor.

All employees should take special note that, as stated above, retaliation against an individual who has complained about sexual harassment, and retaliation against individuals for cooperating with an investigation of a sexual harassment complaint is unlawful and will not be tolerated by the Commonwealth of Massachusetts.

III. Complaints of Sexual Harassment

If any ITD employee believes that he/she has been subjected to sexual harassment, the employee has the right to file a complaint. This may be done in writing or orally.

If you would like to file a complaint you may do so by contacting ITD's Sexual Harassment Officer, Ellen Wright. The Sexual Harassment Officer is also available to discuss any concerns you may have and to provide information to you about ITD's policy on sexual harassment and ITD's complaint process. The procedures for reporting sexual harassment can be located on the HRD website or by contacting any member of the ITD Human Resource Department.

IV. Sexual Harassment Investigation

When ITD receives a complaint it will promptly investigate the allegation in a fair and expeditious manner. The investigation will be conducted by the Sexual Harassment Officer in such a way as to maintain confidentiality to the extent practicable under the circumstances. The investigation will include a private interview with the person filing the complaint and with witnesses. The Sexual Harassment Officer will also interview the person alleged to have committed sexual harassment. When the investigation is completed, ITD will, to the extent appropriate, inform the person filing the complaint and the person alleged to have committed the conduct of the results of that investigation.

If it is determined that inappropriate conduct has occurred, ITD will act promptly to eliminate the offending conduct, and where it is appropriate will impose disciplinary action.

V. Disciplinary Action

If it is determined that an employee has engaged in inappropriate conduct, ITD will take such action as is appropriate under the circumstances. Such action may range from counseling to termination from employment, and may include such other forms of disciplinary action deemed appropriate under the circumstances.

VI. State and Federal Remedies

In addition to the above, if you believe you have been subjected to sexual harassment, you may file a formal complaint with either or both of the government agencies set forth below. Using our complaint process does not prohibit you from filing a complaint with these agencies. Each of the agencies has a short time period for filing a claim (EEOC - 300 days; MCAD - 300 days).

1. The United States Equal Employment Opportunity Commission ("EEOC") One Congress Street, 10th Floor Boston, MA 02114, (617) 565-3200.
2. The Massachusetts Commission Against Discrimination ("MCAD") Boston Office: One Ashburton Place, Rm. 601, Boston, MA 02108, (617) 994-6000. Springfield Office: 424 Dwight Street, Rm. 220, Springfield, MA 01103, (413) 739-2145

E. ITD HR Policy 2008-02 Effective 10/1/2008: Criminal Offender Record Information (CORI) Policy

Updated 11/1/2010

Whereas Criminal Offender Record Information (CORI) checks are part of a general background check for employment at the Information Technology Division (ITD), the following practices and procedures will generally be followed:

1. CORI checks will only be conducted as authorized by CHSB. All applicants will be notified that a CORI check will be conducted. Applicants will be provided with a copy of the CORI policy. Applicants must sign the CORI form prior to ITD submission to CHSB.
2. An informed review of a criminal record requires adequate training. Accordingly, all personnel authorized to review CORI in the decision-making process will be thoroughly familiar with the educational materials made available by CHSB. Unless otherwise provided by law, a criminal record will not automatically disqualify an applicant. Rather, determinations of suitability based on CORI checks will be made consistent with this policy and any applicable law or regulations.
3. If a criminal record is received from CHSB, the authorized individual will closely compare the record provided by CHSB with the information on the CORI request form and any other identifying information provided by the applicant, to ensure the record relates to the applicant.
4. Applicants will be given a copy of their CORI results. Applicants will not be asked any questions about their CORI until we provide them with a copy of their results. If ITD is inclined to make an adverse decision based on the results of the CORI check, the applicant will be notified immediately. The applicant shall be provided with a copy of the criminal record and the organization's CORI policy, advised of the part(s) of the record that make the individual unsuitable for the position or license, and given an opportunity to dispute the accuracy and relevance of the CORI record.
5. Applicants challenging the accuracy of the CORI record shall be provided a copy of CHSB's ***Information Concerning the Process in Correcting a Criminal Record***. If the CORI record provided does not exactly match the identification information provided by the applicant, ITD will make a determination based on a comparison of the CORI record and documents provided by the applicant. ITD may contact CHSB and request a detailed search consistent with CHSB policy.
6. If ITD reasonably believes the record belongs to the applicant and is accurate, based on the information as provided in section 4 of this policy, then the determination of suitability for the position will be made. Unless otherwise provided by law, factors considered in determining suitability may include, but not be limited to the following:

   (a) Relevance of the crime to the position sought; - the following list includes categories of crimes for which conviction will result in disqualification for ITD employment:

   - Violation of any state or federal law or regulation pertaining to data security and/or privacy, including, without limitation and for example, the Fair

Information Practices Act, Mass. Gen. L. ch. 66A , and the privacy and security provisions of the Federal Health Information Portability and Accountability Act ("HIPAA").

ii Violation of the state wiretap law, Mass. Gen. L. ch. 272, sec. 99, or its Federal counterpart, 18 U.S.C. sec. 2511.

iii Violation of Federal or State laws specific to computer crime, including without limitation and for example, the Federal Computer Fraud and Abuse Act, 18 U.S. C. sec. 1030 and the Massachusetts state law prohibiting electronic transmission of threats, Mass. Gen. L. ch. 269, sec. 14.

iv Violation of any state criminal laws if follow up communication with applicant discloses that information technology (computers, networks, and peripheral devices) was used to commit the acts on which the conviction was based. The following are examples of state laws under which crimes committed using computers could theoretically be prosecuted: Mass. Gen. L. ch. 272, sec. 29B (dissemination of child pornography); Mass. Gen. L. ch. 272 sec. 29C (possession of child pornography); Mass. Gen. L. ch. 265, sec. 43 (stalking) and 43A (harassment). Mass. Gen. L. ch. 275 s. 2 (threat to commit crime); Mass. Gen. L. ch. 266 sec. 30 (larceny statute used in hacking and other data theft cases); Mass. Gen. L. ch. 266, sec. 12 (willful and malicious destruction of property, for use in website defacement and other hacking cases); Mass. Gen. L. ch. 266, sec. 30 (theft of intellectual property).

v Violation of laws pertaining to trade secrets, copyrights, patents, or any other form of protection of intellectual property.

vi Violation of state criminal laws pertaining to theft, fraud, misrepresentation, tax evasion, and other forms of white collar crime.

vii Violation of state law pertaining to unauthorized access (MGL ch. 266 s. 120F) and identity fraud, MGL ch. 266, s. 37E

(b) The nature of the work to be performed;

(c) Time since the conviction;

(d) Age of the candidate at the time of the offense;

(e) Seriousness and specific circumstances of the offense;

(f) The number of offenses;

(g) Whether the applicant has pending charges;

(h) Any relevant evidence of rehabilitation or lack thereof;

(i) Any other relevant information, including information submitted by the candidate or requested by the hiring authority

7. ITD will notify the applicant of the decision and the basis of the decision in a timely manner.
8. Applicants challenging the relevance of their CORI record to an adverse decision may submit a letter to the Director of Human Resources within 3 business days of receipt

of notification of non-selection, specifying why they believe their CORI record is not relevant to the position for which they are applying.

9. Access to CORI results will be limited to the following ITD staff members: Payroll Manager, Director of Human Resources, and General Counsel. The Payroll Manager will maintain a record of all CORI requests submitted and document dates and names of individuals receiving copies of CORI results. If an offer of employment is extended to an employee, the Director of Human Resources will return all copies of CORI results to the Payroll Manager and the Payroll Manager will document date copies were returned, destroy all copies produced, and record date that records were destroyed. If a decision is made not to extend an offer of employment based on CORI results, Director of Human Resources and General Counsel will return all copies of CORI results to Payroll Manager. The Payroll Manager will record dates that copies were returned. In addition, the Payroll Manager will maintain a file for all candidates who were not extended an offer of employment based on CORI results, including a copy of the CORI results for each candidate. This file will be stored in a locked file cabinet and maintain per required document retention schedule.

F. ITD HR Policy 2006-02 Updated 9/1/2010: Telecommuting Policy

Updated 9/1/2010

Policy

It is the policy of the Information Technology Division to facilitate, in appropriate circumstances, telecommuting opportunities for its employees.

Definition of Telecommuting

Telecommuting is a form of telework, which is the use of telecommunications technology to work from any remote location. In most instances, it is the act of working from home, thus eliminating travel to and from an office. Some jobs have tasks that could be accomplished while telecommuting one or at most two days per week or on an ad hoc, project-specific basis. Generally, jobs suitable for telecommuting will have defined tasks with clearly measurable results. Ultimately, whether or not management decides to utilize telecommuting as an option will depend on the operational needs of the agency or operating unit.

Limitations/Benefits of Telecommuting

Limitations of telecommuting can include:

The potential for distractions at home
Reduced exposure and interaction with coworkers
Lack of supervisory control
Difficulty in locating telecommuters during work hours
Should not be a substitute for primary childcare or eldercare arrangements

Benefits of telecommuting can include:

Increased productivity (including better time management and work quality)
Improved employee morale (including a better work/family balance)

Telecommuting Program Criteria

The decision to allow or continue a telecommuting program is at the sole discretion of the Information Technology Division's Agency head – the "Appointing Authority".. Additionally, the decision to approve or continue an individual telecommuting arrangement must go through review and approval of ITD Human Resource Governance Board. In terms of supervision, clear expectations and measurable tasks are essential components in considering whether or not telecommuting would be an option. Management must supervise telecommuting employees by developing a system of distributing work appropriate for telecommuting and designating tasks with measurable outputs that can ensure appropriate levels of employee accountability.

Individuals eligible for telecommuting must:

Have more than six month's experience at ITD, and have received a rating of meets or above in each category in their latest EPRS evaluation. Eligible employees must not require close supervision or on the job training, and must be the type of employee that can work effectively in an isolated setting.

Have a current form 30 in their personnel file that specifies that their job function may be eligible for consideration for telecommuting.

Be organized, highly disciplined, conscientious, motivated self-starters who require minimal supervision and consistently meet or exceed deadlines assigned to them.

Be members of bargaining unit or management positions at ITD. **Hourly contractors to ITD are not eligible for telecommuting.**

Additionally, supervisors or managers of employees who require close supervision, as determined by the HR Governance Board, are not eligible for regularly scheduled telecommuting.

Telecommuting Program Elements

ITD's Telecommuting Coordinators are Jennifer Magrone and LaRoyce Jacks. Jennifer will be responsible for employees at the Data Center and LaRoyce will be responsible for employees in Boston.

The Telecommuting Coordinators will provide employees with copies of and information about ITD's telecommuting policy; ensure compliance with ITD's telecommuting policy; provide supervisor, telecommuter and coworker orientation; periodically audit the use of the telecommuting policy; and fulfill such other responsibilities as are deemed appropriate by the Appointing Authority. In addition, the Telecommuting Coordinators will act as a resource for telecommuting employees and address their questions and problems.

The decision to approve or continue an individual telecommuting arrangement is at the sole discretion of HR Governance Board. The HR Governance Board may discontinue a telecommuting arrangement at any time if continuation would not be productive, efficient or otherwise not in ITD's best interest.

Managers of telecommuting employees shall supervise the work product produced by employees on telecommuting days to ensure appropriate levels of employee accountability. Managers will require an approved written work plan be submitted to the immediate supervisor/manager prior to the telecommuting date/s of service. Once telecommuting is complete, the employee must reconcile the submitted work plan with what was actually completed and make any necessary changes/ adjustments and submit to immediate supervisor/manager as verification and accountability of telecommuting dates of service.

Individual employees may not regularly telecommute for more than 20% of their work schedule in a given week. For employees who work a five day schedule, they may telecommute one day per week as long as that does not exceed 20% of their work schedule. Employees on a compressed work schedule, working full time in fewer than five days per week, are not eligible to telecommute one day per week if that day represents more than 20% of their work schedule.

Individuals approved for 'ad hoc' telecommuting should be limited to one telecommuting day per month unless an emergency situation (weather, DR) requires additional telecommuting time.

Telecommuting employees must sign a "telecommuting agreement" between ITD and the employee outlining the specific rules and guidelines of their telecommuting arrangement.

A copy of the ITD telecommuting agreement is attached hereto as Exhibit A and the signed original is kept on file with the Telecommuting Coordinator.

Consistent with ITD's Remote Access and VPN Policy, ITD will, in most cases, provide access to and support for VPN and the network. VPN users will be able, in most cases, to access the same applications and data as they would in their office. The telecommuter will be responsible for providing hardware and connectivity to the Internet at their remote location, as well as maintenance and support. The network, VPN and ITD applications and data are Commonwealth information technology resources (ITRs). With the exception of VPN and ITD's network, employees are responsible for the equipment, software, and connectivity required by them to telecommute. At the sole discretion of managers, and subject to the availability of spare equipment, managers may provide some users with portable PCs. If employee is provided with a laptop, the "Offsite Equipment Use Policy" needs to be signed, approved by immediate supervisor/manager and returned to the VPN Coordinator. This ensures the employee is accountable for Commonwealth equipment as all equipment is inventoried and leased.

Telecommuters must comply with all provisions of ITD's Remote Access and VPN Policy, including ITD's rules regarding the security and confidentiality of Commonwealth data and information.

Telecommuters must comply with the Executive Office for Administration and Finance's Acceptable Use Policy with respect to the Commonwealth's Information Technology Resources when telecommuting.

Employees who choose to participate in the telecommuting program shall be responsible for adhering to this policy.

Contractual Rights.

Employee participation in telecommuting under this policy is voluntary. However, nothing in the Commonwealth's Telecommuting Policy or ITD's Telecommuting Policy shall be deemed to abrogate or mitigate any employee or employer contractual rights as they relate to the staffing or assignment of personnel.

Telecommuter Agreement

This Agreement does not constitute a contract for employment or a modification of any other existing terms and conditions of employment between the employee and the employer. The employee affirms that he/she has read and fully understands the Information Technology Division's Telecommuting Policy, which is hereby incorporated and made part of this Agreement.

Except as agreed to in this individual "Telecommuter Agreement", employee rights provided for in the employee's collective bargaining agreement are not affected by participation in a telecommuting program. Rights or benefits provided under the employee's collective bargaining agreement between the Commonwealth and the employee labor unions are neither enhanced nor abridged by the implementation of a telecommuting arrangement.

This Telecommuter Agreement is between the Information Technology Division and the telecommuter employee, (hereinafter "ITD" and "telecommuter").

I. Hours and Days of Work

1. All work schedules require management approval. Changes in work schedules or temporary telecommuting assignments may be made at ITD's discretion to meet management needs or to accommodate an employee's request. Additionally, any temporary modification or change to the designated telecommuting day(s) must be mutually agreed upon by the telecommuter and his/her supervisor, and documented in an email from the supervisor to the employee with a copy to the Telecommuting Coordinator specifying the schedule change and the manner in which the supervisor approved such change. This documentation must be completed for any "ad hoc" telecommuting day approved by a supervisor.
2. Certain meetings are mandatory and will require the telecommuter to come into a work location specified by ITD. Advance notice of such meetings will be given to the extent possible.
3. The telecommuter will follow timekeeping and reporting requirements established by ITD. Specifically, telecommuting employees shall timely enter data in Clarity for telecommuting days in the same manner as they enter such data for non-telecommuting days (i.e. by 10:00am. each Friday unless requested to file earlier). Employees who do not use Clarity to keep track of their workday in detail shall keep a log of the time worked during telecommuting days and the specific tasks on which they worked during such times. Such log shall be emailed to the telecommuter's supervisor at the end of each telecommuting day.

4. The telecommuter's work hours and designated telecommuting days will be the following:

TELECOMMUTE WORK SCHEDULE

WORK HOURS	WORK DAYS

5. The Telecommuter must be available by phone during the core business hours of 9:00 a.m. to 3:00 p.m. except when a later shift is required for operational needs.
6. Overtime is any time worked over 37.5 hours. Overtime must be authorized in advance by management. Requests for any eligible compensatory time off must be authorized by management in advance.
7. Telecommuters will not provide primary care during designated telecommuting hours for children or elders who would otherwise require a provider's care.

II. Work Site

8. Failure to maintain a proper and safe work environment, in accordance with this Agreement, may be cause for terminating an employee from the telecommuting program. A proper and safe work environment is defined as taking care to ensure that home office equipment (computers, printers, fax machines, lighting) do not overload electrical circuits, that circuit breakers and surge protectors are used when necessary, and that walkways are clear of debris and electrical cords. ITD retains the right to make an on-site inspection of the designated workspace at a mutually agreed upon time.
9. The telecommuter is responsible for the safety and security of ITD's equipment, software, data and supplies in accordance with the Information Technology Division's guidelines.
10. If an employee incurs a work-related injury while telecommuting, workers' compensation laws and rules will apply just as they would if such an injury occurred at the regular work site.
11. ITD is not liable for any damages to the telecommuter's property that may result from participation in this telecommuting arrangement.

12. The telecommuter designates the following address as his/her "telecommuting work location", subject to the terms and conditions of this Agreement:

13. (Employee address)_____

III. Work Products, Equipment & Expenses

14. Work products and programs developed by the telecommuter during days and hours designated in this agreement for telecommuting, whether created using the Commonwealth's Information Technology Resources ("ITRs") or the telecommuter's software, hardware or other equipment, remain the property of ITD.

15. ITD may provide access to its network through VPN. Consistent with ITD's VPN policy, . VPN users will be able, in most cases, to access the same applications and data as they would in their office. The telecommuter will be responsible for providing hardware and connectivity to the Internet at their remote location, and maintenance and support therefore. The network, VPN and applications and data are Commonwealth ITRs.

16. Commonwealth equipment and services are to be used for state business only. The use of ITR's shall be in accordance with the Executive Office of Administration and Finance's Acceptable Use Policy with respect to the responsibilities of the employee, acceptable and unacceptable uses of ITR's, data confidentiality, copyright protection, computer viruses, network security, e-mail and employee expectations of privacy.

17. Subject to the terms of ITD's VPN Policy, installation, maintenance, repair or replacement of employee owned equipment and software is the responsibility of the employee. In the event of ITR malfunction, or malfunction of the telecommuter's hardware, software or connectivity, the telecommuter must contact his/her supervisor as soon as possible. If repairs will take some time, the telecommuter may be required to report to a work location specified by ITD until the ITR is usable. In all cases, whether the malfunction is caused by the problems with ITD ITRs or the user's hardware, software or connectivity, the telecommuter must make up the time lost due to the malfunction as soon as possible following such event.

18. The following Equipment Inventory identifies equipment and software which has been provided by _____ to the above-named telecommuter for his or her telecommuting purposes:

EQUIPMENT INVENTORY

Item Description	Serial Number

19. ITD will not pay for the following expenses:

Maintenance or repairs of privately owned equipment

Utility costs associated with the use of the computer or occupation of the home, including but not limited to, electricity and personal phone usage

Connectivity (i.e. the telecommuter's access to the Internet through a commercial service such as Verizon)

Equipment supplies (which should be requisitioned through ITD) and

Travel expenses associated with commuting to the central office.

20. ITD will not pay long-distance phone bills or dial-up access fees incurred by telecommuters.

This Agreement shall become effective when signed by the employee and his/her supervisor and shall remain in effect unless terminated by either party or extended upon mutual written agreement by both parties. This Agreement may be terminated by either party at any time, provided there is written notice of the Agreement's termination.

The following signature of the employee and his/her supervisor indicates that each has read and understands this Agreement and agrees to abide by the terms and conditions contained herein.

_____	_____	_____
Employee Name Printed	Employee Signature	Date
_____	_____	_____
Supervisor Name Printed	Supervisor Signature	Date
_____	_____	_____
HR Gov. Board Approver Printed	HR Gov. Board Approver Signature	Date

G. ITD HR Policy 2008-04 Updated 7/1/2010: Desktop Unit Management Policy

Effective 11/10/2008

Updated April 21, 2009

Updated July 1, 2010

Purpose

The purpose of this policy is to establish a standard for the proper usage of ITD standard software, Desktop hardware and Domain Administration, as managed by the ANF LAN Team.

Scope

The scope of this policy includes all enterprise desktop computers, monitors and operating systems at the ITD Data Center in Chelsea and Boston Office locations.

Policy

1. Employees must not change LAN assigned configuration settings.
2. The assigned computer name may not be changed for any reason. Naming convention for PCs will be as follows: "ANF-(Date of Lease Expiration)-xxxxx", for example, "ANF-10/13-01286".
3. All desktops will have LAN domain administrative accounts.
4. Employees will be held responsible for all components deployed with the computer; for example, PC with monitor (which includes memory, hard drive, DVD/CD combo unit, optical mouse, keyboard etc).
5. Employees must obtain approval of their direct supervisor prior to submitting a request to the ANF LAN Team for administrative rights to the desktop, desktop moves and relocation of the assigned desktop unit.
6. Employees must not move an assigned desktop to a new location or group without approval of the LAN and DESKTOP Manager or his assignee.
7. No downloading is allowed of music, video or other non-work related media files to an ANF desktop.
8. No peer to peer network sharing software is allowed. (for example, but not limited to Kazaa, Napster or BitTorrent)
9. No use of personal, web-based email is allowed from ANF desktops. (for example, but not limited to, yahoo, hotmail or gmail accounts)
10. No non-work related streaming video or audio is allowed.

Enforcement

Any person found to have violated this policy may be subject to appropriate disciplinary action, up to and including termination.

H. ANF Policy on the Use of Information Technology Resources Issued by ANF June 16, 1998

This document formalizes the policy for employees and contractors ("users") of all agencies under the Executive Office for Administration and Finance on the use of information technology resources; ("Agency ITRs"), including computers, printers and other peripherals, programs, data, local and wide area networks, and the Internet. In addition to this policy, individual agencies may choose to issue additional policies governing the use of Agency ITRs. Use of Agency ITRs by any employee or contractor shall constitute acceptance of the terms of this policy and any such additional policies.

1. User Responsibilities

It is the responsibility of any person using Agency ITRs to read, understand, and follow this policy. In addition, users are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of ITRs. Any person with questions regarding the application or meaning of this policy should seek clarification from appropriate management. Failure to observe this policy may subject individuals to disciplinary action, including termination of employment.

2. Acceptable Uses

The Executive Office for Administration and Finance firmly believes that ITRs empower users and make their jobs more fulfilling by allowing them to deliver better services at lower costs. As such, employees and contractors are encouraged to use ITRs to the fullest extent in pursuit of their Agency's goals and objectives.

3. Unacceptable Uses of Agency ITRs

Unless such use is reasonably related to a user's job, it is unacceptable for any person to use Agency ITRs:

in furtherance of any illegal act, including violation of any criminal or civil laws or regulations, whether state or federal

for any political purpose

for any commercial purpose

to send threatening or harassing messages, whether sexual or otherwise

to access or share sexually explicit, obscene, or otherwise inappropriate materials

to infringe any intellectual property rights

to gain, or attempt to gain, unauthorized access to any computer or network

for any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs

to intercept communications intended for other persons

to misrepresent either the Agency or a person's role at the Agency

to distribute chain letters

to access online gambling sites or

to libel or otherwise defame any person.

4. Data Confidentiality

In the course of performing their jobs, Agency employees and contractors often have access to confidential or proprietary information, such as personal data about identifiable individuals or commercial information about business organizations. Under no circumstances is it permissible for employees or contractors to acquire access to confidential data unless such access is required by their jobs. Under no circumstances may employees or contractors disseminate any confidential information that they have rightful access to, unless such dissemination is required by their jobs.

5. Copyright Protection

Computer programs are valuable intellectual property. Software publishers can be very aggressive in protecting their property rights from infringement. In addition to software, legal protections can also exist for any information published on the Internet, such as the text and graphics on a web site. As such, it is important that users respect the rights of intellectual property owners. Users should exercise care and judgement when copying or distributing computer programs or information that could reasonably be expected to be copyrighted.

6. Computer Viruses

Users should exercise reasonable precautions in order to prevent the introduction of a computer virus into the local area or wide area networks. Virus scanning software should be used to check any software downloaded from the Internet or obtained from any questionable source. In addition, executable files (program files that end in ".exe") should not be stored on or run from network drives. Finally, it is a good practice to scan floppy disks periodically to see if they have been infected.

7. Network Security

Most desktop computers are connected to a local area network, which links computers within the Agency and, through the wide area network, to most other computers in state government. As such, it is critically important that users take particular care to avoid compromising the security of the network. Most importantly, users should never share their passwords with anyone else, and should promptly notify Agency MIS personnel if they suspect their passwords have been compromised. In addition, users who will be leaving their PCs unattended for extended periods should either log off the network or have a password protected screen savers in operation. Finally, no user is allowed to access the Internet or other external networks via modem unless they have received specific permission from Agency MIS personnel.

8. E-mail

When using e-mail, there are several points users should consider. First, because e-mail addresses identify the organization that sent the message (first.last@state.ma.us), users should consider e-mail messages to be the equivalent of letters sent on official letterhead. For the same reason, users should ensure that all emails are written in a professional and courteous tone. Finally, although many users regard e-mail as being like a telephone in offering a quick, informal way to communicate, users should remember that e-mails can be stored, copied, printed, or forwarded by recipients. As such, users should not write

anything in an e-mail message that they would not feel just as comfortable putting into a memorandum.

9. No Expectation of Privacy

Agency ITRs are the property of the Commonwealth of Massachusetts and are to be used in conformance with this policy. The Agency retains, and when reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, the Agency will exercise the right to inspect any user's computer, any data contained in it, and any data sent or received by that computer. Users should be aware that network administrators, in order to ensure proper network operations, routinely monitor network traffic. Use of Agency ITRs constitutes express consent for the Agency to monitor and/or inspect any data that users create or receive, any messages they send or receive, and any web sites that they access.

Information Technology User Responsibility Agreement

USER NAME: _____

I, _____, hereby agree to the following terms and conditions governing my use and possession **of a UAID and/or Agency Network Log-in ID.**

1. My UAID and/or Agency Network Log-in ID were issued to me exclusively for the purpose of enabling me to perform my job duties as an employee or contractor of the Commonwealth of Massachusetts. My UAID will allow me to use one or more statewide systems such as HR/CMS, MMARS, the Information Warehouse, MAGIC and ViewDirect to which I have been explicitly granted access. My Agency Network Log-in ID will enable me to use the Commonwealth's Information Technology Resources ("IT Resources") to which I have been granted access for additional purposes. My UAID and/or Agency Network Log-in ID are referred to hereafter as "Log-in IDs".
2. I must keep my Log-in IDs and corresponding passwords confidential, and not knowingly allow anyone else to use them for any reason. I must not disclose my Log-in IDs to anyone, including my coworkers and administrative assistants. I must not record and store my Log-in IDs and passwords in a manner that makes them accessible to others, or e-mail them to anyone.
3. When I choose my password, I must not choose a variation on my Log-in IDs, my first, middle, or last names (current or former); the names of my immediate family members; or other information easily obtainable about me (license plate number, telephone number, social security number, automobile brand, street name). I must choose a password that is easy for me to remember so that I don't have to write it down.
4. Use of my Log-in IDs is a privilege that can be revoked for failure to comply with the terms of this agreement
5. I am solely responsible for my Log-in IDs and corresponding passwords. This means that I can be held accountable for any access gained and/or any transactions attempted or completed with my Log-in IDs and corresponding passwords by me or anyone else who gains access to the Commonwealth's IT Resources as a result of my negligence in failing to safeguard this information. I must immediately report to my department or agency security officer any information that would lead a reasonable person to believe that someone else other than me had obtained access to my Log-in IDs and corresponding passwords.
6. I am not authorized to allow anyone to have access to, and I am not authorized to release, any information or data held in the Commonwealth's IT Resources and accessible to me through the use of my Log-in IDs and passwords except in a manner consistent with the laws, regulations and policies that govern my agency.

7. I may have the opportunity to access the Commonwealth's IT Resources remotely, using authorized remote access methods such as VPN or Web-based processes such as Outlook Web Access. I understand that remote use of the Commonwealth's IT Resources multiplies the possibilities for inadvertent disclosure of the Commonwealth's confidential data. Passersby eavesdropping over my shoulder, passengers sitting next to me on an airplane, or family members in my home could have inappropriate (and in some cases illegal) access to the Commonwealth's confidential data similar to that which would occur if I removed such information from my office and left it in plain view of the public. Remote access to the Commonwealth's IT Resources poses the same or greater risks than offsite use of paper resources containing such data. When accessing the Commonwealth's data remotely using any authorized technology, I will take extra precautions to ensure that my use does not compromise the confidentiality of the Commonwealth's data or the privacy of individuals and other entities to whom such information pertains. Such extra precautions include, but are not limited to, shielding the screen of my remote access device (laptop, PC, or PCD) from others, and logging off if I leave such device out of my sight and in the view of others during a work session. My agency's remote access policy specifies additional restrictions on remote access. I understand that my Log-in IDs can be revoked if I violate the terms of my agency's remote access policy.
8. I understand that improper use of or negligence in safeguarding my Log-in IDs and passwords and Commonwealth IT Resources to which I have access as a result of my possession of these identifiers will result in my agency's suspension of my use of these identifiers. If I am an employee, improper use of or negligence in safeguarding such information, and any other violation of this IT User Responsibility Agreement, may subject me to disciplinary action up to and including termination. If I am a contractor, such use may result in termination of my contract. Whether I am an employee or contractor, such use, negligence or violations may expose me to civil liability and criminal fines and imprisonment.
9. I have read and understand my agency's acceptable use policy, a copy of which is attached hereto. My continued use of my Log-in IDs and passwords is contingent upon my compliance with my agency's acceptable use policy.
10. I understand that incoming and outgoing e-mails are screened by ITD for viruses and "spam", and may be screened for profanity (specifically, offensive ethnic, racial or sexual language).
11. If I have any questions concerning the security or use of my Log-in IDs and passwords, I understand that I may contact my departmental security officer, _____.

I, the user, have read and understand this Information Technology User Responsibility Agreement governing the use of the Log-in ID assigned to me.

_____

User Name (Please Print)

_____

Signature

_____

Date

I. Enterprise Information Technology Policies

The following review and summary of Enterprise Information Technology Policies has been prepared to assist users in upholding their responsibility for understanding the kind of information they handle and knowing what policies apply to that information. Questions regarding your security access may be directed to your managers. Questions regarding enterprise policies may be directed to ITD's Enterprise Policy Group.

Enterprise Information Technology policies are high level documents that specify requirements and rules. These mandatory and enforceable directives are often supported by functional Standards, technical Standards, and Architecture documents that provide additional compliance requirements.

Enterprise Policies must be adhered to by any entity within the Commonwealth of Massachusetts' Executive Department. This includes but is not limited to:

- Support Staff
- Staff responsible for purchasing every day items
- Staff responsible for purchasing and/or approving applications or other technical appliances
- Technical Staff
- Management Staff
- Staff responsible for overseeing external agency activity in some way, i.e. Security Assessment & Design Team

Everyone within Executive Department Agencies is responsible for complying with all Enterprise Policies and Standards as applicable. Enterprise Policies and Standards can be found on the ITD section of the ANF website, www.mass.gov/anf, click on center section "Research & Technology", then click on "Policies, Standards & Guidance" then choose the link to "Enterprise Policies & Standards".

The complete list of Enterprise Policies and Standards as of the date of publication of this handbook follows:

- Enterprise Technical Reference Model (ETRM)
- Information Technology Architecture and Enterprise Standards (SOE)
- Acceptable Use of Information Technology Resources(EOAF)
- Enterprise Information Technology Acquisition Policy
- Enterprise Information Technology Accessibility Standards
- Enterprise Web Accessibility Standards
- Enterprise Open Standards Policy
- Enterprise Information Security Policy
- Enterprise Information Security Standards: Data Classification
- Enterprise Cybercrime Security Incident Policy
- Attack Intrusion Notification Procedures
- Enterprise Desktop Power Management Standards
- Enterprise Electronic Messaging Communications Security Policy
- Enterprise Public Access Policy for e-Government Applications

- Enterprise Public Access Standards for e-Government Applications: Application Security
- Enterprise Public Access Standards for e-Government Applications: Network Security
- Enterprise Remote Access Security Policy
- Wireless Security Policy
- Wireless Security Standards: Wireless Local Area Networks
- Wireless Security Standards: Wireless Mobile Communications
- Wireless Security Standards: Wireless Personal Area Networks
- Wireless Security Standards: Wireless Wide Area Networks
- The Commonwealth's Web Site Privacy Policies
- Requirements for Agency Website Privacy Policies
- Privacy Policy Requirements (Additional Guidance)

The following Enterprise policies are generally applicable to all types of users of Information Technology Resources and are provided to highlight specific topics of concern to all users. However, it is the responsibility of the individual to comply with any policies that apply regardless of whether or not is has been highlighted here:

- Information Security Policy
- Acceptable Use of Information Technology Resources (EOAF)
- Enterprise Cybercrime & Security Incident Response Policy and Procedures
- Enterprise Desktop Power Management Standards
- Enterprise Electronic Messaging Communications Security Policy
- Enterprise Remote Access Policy
- Enterprise Wireless Policy & related Standards
- Enterprise Web Accessibility Standards

Information Security Policy

This policy specifies agency's responsibilities for developing information security policies and procedures within their entity. The practices articulated within this policy will ensure that the integrity, confidentiality, and availability of information and allow for the enforcement of proper controls including: Access Cards, User ID & Password, Sign-In policy, Escort policy, etc.

Key requirements of this policy include:

- All employees need to understand what kind of information they possess or have access to; what risks there are to the information; and how it should be safeguarded and used.
- Agency adoption and implementation of an acceptable use policy for all Information Technology Resources
    - ITD requires all users to comply with the ANF Acceptable Use Policy and sign the User Responsibility Agreement. These documents are both included in Section Two of the ITD Workplace Policies and Procedures Guide.

- Enforcement of Paragraph Six of the Commonwealth's Terms & Conditions specifying that Contract Employees are responsible for protecting the physical security of and access to department data that they have possession of or access to.

Acceptable Use of Information Technology Resources (EOAF)

The acceptable use policy formalizes the acceptable uses of information technology resources (ITR's) for all EOAF agencies and contractors and applies to use of computers, printers, other peripherals, data, local and wide area networks, and the internet. All individuals should make themselves fully aware of all requirements and prohibitions set forth in this document.

Enterprise Cybercrime & Security Incident Response Policy and Procedures

Cybercrime & Security Incidents are defined as internally or externally initiated events, intentional or accidental, which threaten or exploit an unauthorized and/or illegal use of Commonwealth electronic information systems and/or services.

Such events include, but are not limited to, a criminal use of Commonwealth systems and/or services (e.g., cyber-stalking, identity theft, child pornography, etc.) as well as disclosure, destruction, and/or alteration of state managed systems or data.

In the event that you are victim of a Cybercrime or Security Incident:

- Immediately report it to Commonhelp and await further instruction.
- Do not open emails with suspected viruses.
- Do not delete emails with threatening or obscene content until you've received direction from Commonhelp to do so.
- Do not forward emails to anyone unless you've received direction from Commonhelp or the Security Response Team to do so.

Enterprise Desktop Power Management Standards

The Enterprise Desktop Power Management Standards provide the minimum requirements for optimizing power consumption among the Commonwealth of Massachusetts' PCs and workstations.

Key points from this policy include:

- Identifies and explains the requirements agencies must apply to achieve the appropriate power management controls for the following scenarios: basic, remote desktop, special purpose and new workstations.
- Requires agencies to purchase, lease and dispose of workstations and peripherals in compliance with the Operational Services Division policies and procedures.
- Information about the relevant national standards and definitions that are commonly referred to when discussing computer power management practices and standards.

The Enterprise Electronic Messaging Communications Security

The Enterprise Electronic Messaging Communications Security Policy identifies current controls that are in place to protect the Enterprise from threats generated by e-mails.

Key points from this policy include:

- Enterprise Filtering: All inbound and outbound email is filtered for known viruses, spam, message syntax and message segmentation.
- Private email accounts are not allowed within MAGNet, which means that users are prohibited from accessing browser-based email accounts such as yahoo and gmail.
- Instant Messaging is prohibited within MAGNet.

ITD employees must comply with prohibitions and specifications of this policy.

Remote Access Policy

The Enterprise Remote Access policy specifies requirements and acceptable methods for remote access to the WAN and all Commonwealth IT domains.

Agencies are responsible for implementing their own Remote Access policy to address the following key points:

- Employees need to understand the risks associated with transfer of confidential or sensitive information from a Remote Access point.
- Employees need to adhere to any and all security controls based on the classification of the data that is accessed remotely.
- Users are responsible for safeguarding passwords and understand response plan for loss or compromise of passwords.
- Users need to adhere to measures taken to secure the remote access sessions, including requiring that users deploy and maintain anti-virus software and personal firewall software as specified.
- Users must sign a Remote Access agreement provided by their agency.

ITD has issued its own Remote Access Policy, included in Section Two of this handbook. If you currently have or expect to have Remote Access, make sure you understand what your responsibilities are as identified in the user agreement you will be asked to sign.

Enterprise Wireless Policy & Related Standards

The Enterprise Wireless Policy and related Standards address potential security problems with prospective and actual wireless implementations, sets requirements to ensure the best possible security is implemented, and to preclude the use of wireless technology when security cannot be ensured.

The Wireless Policy and Related Standards include the following documents:

- Enterprise Wireless Security Policy
- Enterprise Wireless Security Standards: Wireless Personal Area Networks
- Enterprise Wireless Security Standards: Wireless Wide Area Networks
- Enterprise Wireless Security Standards: Wireless Local Area Networks
- Enterprise Wireless Security Standards: Wireless Mobile Communications

Key points from this policy include:

- Wireless devices must be registered prior to connecting to LANs or WLANs. Information must be provided to ITD upon request.
- Wireless devices must be the property of the Commonwealth if connecting to LANs or MAGNet.

- Agency must maintain administrative control over the devices.
- Devices that may contain confidential data must have a first tier authentication for device access (login and password).
- Transmission of confidential data is prohibited via WPAN connections.
- Access to the LAN or MAGNet is prohibited via WPAN connections.
- Devices must be configured in compliance with the Commonwealth's Enterprise security policies, e.g. updated anti-virus software, patched, personal firewalls, etc.
- Peer-to-Peer communication between wireless devices is prohibited.
- Access to LAN/MAGNet resources from wireless devices must utilize an ITD-approved VPN solution to protect transmission end-to-end and must use two factor authentication (certificate and pasword; secureID card and password, etc.)
- Any browser enabled device must use, at a minimum, SSL 128bit encryption.

Any ITD employee using wireless devices of any kind must be aware of the Wireless Policy and Related Standards and comply with requirements and prohibitions of these documents.

Enterprise Web Accessibility Standards

The purpose of the Web Accessibility Standards is to ensure access to state web pages for everyone.

Key points from this policy include:

- Forms designed to be completed online and other interactive interfaces must be accessible by people using assistive technology.
- Web pages must provide a text equivalent for every non-text element.
- Web pages must provide synchronized auditory and readable text descriptions of the important information of the visual track of a multimedia presentation.
- Web pages that use motion must ensure the motion is integral to the content of the site, user-controlled, and limited to three cycles and then stopped automatically.
- Use and selection of color cannot affect the information conveyed on the page.
- All information published on web pages must be published in HTML, whenever possible.
- Files downloadable from a web page in a compressed format must also be provided in its uncompressed format or as a self extracting file.
- Files must be optimized to improve download time.
- Web accessibility statement must be linked to the web page.
- Agencies must validate web content against these Standards prior to posting and at regular intervals after posting.
- Appendices: Sample Web Accessibility Statement, Web Accessibility Standards Checklist, Related Standards.

Any ITD employee involved with web development must be aware of the Web Accessibility Standards and comply with requirements and prohibitions of the standards.

This page intentionally left blank.

Commonwealth of Massachusetts

Information Technology Division
Workplace Policies and Procedures Guide
Signature of Receipt

I have received a printed copy of the Information Technology Division Workplace Policies and Procedures Guide on the date indicated below. My signature indicates acknowledgement that I did receive this document.

Name (Printed)

Signature

Date